# SIMULTANEOUS APPROXIMATION BY CONJUGATE ALGEBRAIC NUMBERS IN FIELDS OF TRANSCENDENCE DEGREE ONE

DAMIEN ROY

Abstract. We present a general result of simultaneous approximation to several transcendental real, complex or p-adic numbers $\xi_1, ..., \xi_t$ by conjugate algebraic numbers of bounded degree over $\mathbb{Q}$, provided that the given transcendental numbers $\xi_1, ..., \xi_t$ generate over $\mathbb{Q}$ a field of transcendence degree one. We provide sharper estimates for example when $\xi_1, ..., \xi_t$ form an arithmetic progression with non-zero algebraic difference, or a geometric progression with non-zero algebraic ratio different from a root of unity. In this case, we also obtain by duality a version of Gel'fond's transcendence criterion expressed in terms of polynomials of bounded degree taking small values at $\xi_1, ..., \xi_t$.

## 1. Introduction

The basic problem of approximation to real numbers by algebraic numbers of bounded degree has attracted much attention since the pioneer work [17] of E. Wirsing in 1961. In their seminal paper [6] of 1969, H. Davenport and W. M. Schmidt proposed an innovative approach based on geometry of numbers which allowed them to deal with approximation by algebraic integers. Recently, Y. Bugeaud and O. Teulié observed that it can also be used to treat approximation by algebraic integers of a fixed degree [1]. The sharpest result in this direction is due to M. Laurent [7, Cor.]. Simplifying slightly, it shows that, for each integer $n \geq 2$ and each real number $\xi$ which is not algebraic over $\mathbb{Q}$ of degree at most $n/2$, there are infinitely many algebraic integers $\alpha$ of degree $n$ over $\mathbb{Q}$ which satisfy $|\xi - \alpha| \leq \mathrm{H}(\alpha)^{-n/2}$, where the *height* $\mathrm{H}(\alpha)$ of $\alpha$ is defined as the largest absolute value of the coefficients of the irreducible polynomial of $\alpha$ over $\mathbb{Z}$. Similar estimates valid for a $p$-adic number $\xi \in \mathbb{Q}_p$ are also known [11, 16].

The present work deals with the problem of simultaneous approximation to several numbers by conjugate algebraic numbers. Naive heuristic arguments based on Dirichlet box principle suggest that, for each integer $t \geq 1$ and each choice of transcendental real numbers $\xi_1, \ldots, \xi_t$, there exist constants $n_0 \geq 1$ and $c > 0$ with the property that, for each integer $n \geq n_0$, there are infinitely many algebraic numbers $\alpha$ of degree $n$ over $\mathbb{Q}$ which admit distinct real conjugates $\alpha_1, \ldots, \alpha_t$ with $|\xi_i - \alpha_i| \leq \mathrm{H}(\alpha)^{-cn}$ for $i = 1, \ldots, n$. For $t = 1$, this heuristic statement is true, by the above, with $n_0 = 2$ and $c = 1/2$. When $\xi_1 = \cdots = \xi_t$, it is

1991 *Mathematics Subject Classification.* Primary 11J13; Secondary 11J82.

*Key words and phrases.* simultaneous approximation, conjugate algebraic numbers, polynomials, Gel'fond's criterion, heights.

Work partially supported by NSERC and CICMA.

also true with $n_0 = 4t + 1$ and any choice of $c$ with $c < 1/(4t^2)$ by [14, Thm. A]. In general however it is false and the best that one can hope is an exponent of approximation of the form $cn^{1/t}$ instead of $cn$ (see [14, Prop. 10.2]). Our main goal here is to show that the above heuristic statement is true under the restriction that $\xi_1, \dots, \xi_t$ belong to a field of transcendence degree one over $\mathbb{Q}$. Corresponding values that we find for $n_0$ and $c$ are $n_0 = 4Dt^2$ and $c = 1/(4Dt^3)$ where $D$ denotes the degree of an algebraic curve of $\mathbb{C}^t$ defined over $\mathbb{Q}$ and passing through the point $(\xi_1, \dots, \xi_t)$. Although we don't know if $c$ really requires such dependence in $D$ and $t$, we can improve its value to $c = 1/(4Dt^2)$ when $\xi_1, \dots, \xi_t$ are distinct. When they further satisfy a recurrence relation of the form $\xi_{i+1} = a\xi_i + b$ for $i = 1, \dots, t-1$, for some $a, b \in \mathbb{Q}$ with $a \neq 0, -1$ and $(a, b) \neq (1, 0)$, we can even take $n_0 = 4t$ and $c = 1/(4t)$.

As a bi-product of this work, we obtain a version of Gel'fond's transcendence criterion expressed in terms of polynomials of bounded degree taking small values on a fixed sequence of points in arithmetic progression with rational difference or in geometric progression with rational ratio. This new criterion was our original motivation in writing the present paper, and we hope to extend its scope in future work.

In the next section, we state our main results in the more general setting of the previous joint work [14] with M. Waldschmidt. This means that, in order to cover at once the case of approximation to real, complex or $p$-adic numbers, we replace the field $\mathbb{Q}$ with a number field $K$, and the field $\mathbb{R}$ with the completion of $K$ at some place $w$. Our strategy for proving these results follows that of [14] and is again based on the general method of Davenport and Schmidt [6]. It is briefly described in the next section.

## 2. Main results and notation

Throughout this paper, we fix an algebraic extension $K$ of $\mathbb{Q}$, a non-trivial place $w$ of $K$, and an algebraic closure $\bar{K}$ of $K$. We denote by $d$ the degree $[K : \mathbb{Q}]$ of $K$ over $\mathbb{Q}$, by $\mathcal{M}$ the set of all non-trivial places of $K$ and by $\mathcal{M}_\infty$ the subset of $\mathcal{M}$ consisting of all Archimedean places of $K$. For each $v \in \mathcal{M}$, we denote by $K_v$ the completion of $K$ at $v$, and by $d_v$ the local degree $[K_v : \mathbb{Q}_v]$ where $\mathbb{Q}_v$ stands for the topological closure of $\mathbb{Q}$ in $K_v$. We also normalize the absolute value $|\ |_v$ of $K_v$ by asking that, if $v$ is above a prime number $p$ of $\mathbb{Q}$, we have $|p|_v = p^{-d_v/d}$ and that, if $v$ is an Archimedean place, we have $|x|_v = |x|^{d_v/d}$ for any $x \in \mathbb{Q}$. With this convention, the product formula reads $\prod_{v \in \mathcal{M}} |a|_v = 1$ for each $a \in K^\times$, where $K^\times$ stands for the multiplicative group of $K$.

In order to state our main results of approximation, we also precise the following notions. As in the introduction, we define the *height* $\mathrm{H}(\alpha)$ of an algebraic number $\alpha$ to be the largest absolute value of the coefficients of the irreducible polynomial of $\alpha$ over $\mathbb{Z}$. The *rank* of a prime ideal $\mathfrak{p}$ of $K[x_1, \dots, x_t]$ is the largest integer $r \geq 0$ for which there is a strictly increasing chain of $r + 1$ prime ideals in $K[x_1, \dots, x_t]$ ending with $\mathfrak{p}$, and its *degree* is defined to be the degree of the corresponding homogeneous prime ideal of $K[x_0, x_1, \dots, x_t]$. In geometrical

terms, if $V$ denotes the set of zeros of $\mathfrak{p}$ in $\bar{K}^t$, then the rank of $\mathfrak{p}$ is $t-\dim(V)$ and its degree is the degree of the Zariski closure of $V$ in $\mathbb{P}^t(\bar{K})$.

**Theorem 2.1.** *Let $n$ and $t$ be positive integers, and let $\xi_1,\dots,\xi_t$ be elements of $K_w$ for which the field $K(\xi_1,\dots,\xi_t)$ has transcendence degree at most one over $K$. Let $s$ be the number of distinct points among $\xi_1,\dots,\xi_t$, let $m$ be the largest integer for which the sequence $\xi_1,\dots,\xi_t$ contains a point $\xi$ repeated $m$ times, let $\mathfrak{p}$ be a prime ideal of $K[x_1,\dots,x_t]$ of rank $t-1$ whose elements all vanish at $(\xi_1,\dots,\xi_t)$, and let $D$ be the degree of $\mathfrak{p}$. Assume that*

$$n \geq 4Dst \quad \text{and} \quad [K(\xi_i):K] \geq \frac{n}{Dt} \quad (1 \leq i \leq t).$$

*Then, there are infinitely many algebraic numbers $\alpha \in \bar{K}$ which, over $K$, have degree $n$ and admit distinct conjugates $\alpha_1,\dots,\alpha_t$ in $K_w$ satisfying*

$$\max_{1\leq i\leq t} |\xi_i - \alpha_i|_w \leq \mathrm{H}(\alpha)^{-n/(4dDmst)}. \tag{1}$$

In the case where $\xi_1 = \cdots = \xi_t$, we have $s = 1$ and $m = t$, and, as the point $(\xi_1,\dots,\xi_t)$ lies on a rational line, we can take $D = 1$. Then the above result becomes essentially [14, Thm. A]. In this case, [14, Prop. 10.1] shows that the exponent of approximation $n/(4dt^2)$ in (1) is best possible up to the numerical factor $1/4$.

In the case where $\xi_1,\dots,\xi_t$ are distinct elements of $K_w$ which all belong to $K + K\xi_1$, we can take $D = m = 1$ and $s = t$, and then the exponent of approximation in (2.1) again becomes $n/(4dt^2)$. The following result provides a special case where the factor $t^2$ in the denominator can be replaced by $t$.

**Theorem 2.2.** *Let $n$ and $t$ be positive integers, and let $\xi_1,\dots,\xi_t$ be elements of $K_w$ which, for some polynomial $A(T)$ of $K[T]$ of degree one, satisfy the recurrence relation $\xi_{i+1} = A(\xi_i)$ for $i = 1,\dots,t-1$. Assume moreover that $A^i(T) \neq T$ for $i = 1,\dots,n$, where $A^i$ denotes the $i$-th iterate of $A$, and that*

$$n \geq 4t \quad \text{and} \quad [K(\xi_1):K] \geq \frac{n}{t}.$$

*Then, there are infinitely many algebraic numbers $\alpha \in \bar{K}$ which, over $K$, have degree $n$ and admit distinct conjugates $\alpha_1,\dots,\alpha_t$ in $K_w$ satisfying*

$$\max_{1\leq i\leq t} |\xi_i - \alpha_i|_w \leq \mathrm{H}(\alpha)^{-n/(4dt)}.$$

Our last main result is the following version of Gel'fond's transcendence criterion where, for a place $v \in \mathcal{M}$ and a polynomial $Q = \sum_{i=0}^n a_i T^i \in K_v[T]$, we define $\|Q\|_v = \max_{0\leq i\leq n} |a_i|_v$.

**Theorem 2.3.** *Let $n$ and $t$ be positive integers with $n \geq 4t$, and let $\xi_1,\dots,\xi_{n+1}$ be elements of $K_w$. Suppose that there exists a non-zero element $\gamma$ of $K$ such that either we have $\xi_{i+1} = \gamma + \xi_i$ for $i = 1,\dots,n$ (additive case), or we have $\xi_{i+1} = \gamma\xi_i$ for $i = 1,\dots,n$ and $\gamma^i \neq 1$ for $i = 1,\dots,2n$ (multiplicative case). Assume moreover that, for each sufficiently large real*

*number $Y$, there exists a non-zero polynomial $Q \in K[T]$ of degree at most $n$ which satisfies $\|Q\|_v \leq 1$ for each place $v$ of $K$ distinct from $w$ and also*

$$\|Q\|_w \leq Y \quad \text{and} \quad \max_{t+1 \leq i \leq n+1} |Q(\xi_i)|_w \leq Y^{-(4t)/(n+1-4t)}. \tag{2}$$

*Then, $\xi_1, \dots, \xi_{n+1}$ are algebraic over $K$ of degree strictly less than $n/t$.*

Note that the above statement is false if we replace the exponent $(4t)/(n+1-4t)$ in (2) by any exponent smaller than $t/(n+1-t)$ because Dirichlet box principle shows that the hypotheses then become satisfied for any choice of $\xi_1, \dots, \xi_t \in K_w$ (see [14, §3]).

**Outline of the proof.** For the problem of approximation, instead of looking for just one polynomial of $K[T]$ of degree at most $n$ taking small values at the given numbers $\xi_1, \dots, \xi_t$, we follow the idea of Davenport and Schmidt in [6] and look for $n+1$ linearly independent polynomials with this property. Then, it is easy to build out of them an irreducible polynomial of $K[T]$ of degree $n$ taking small values at $\xi_1, \dots, \xi_t$ while some of its derivative at the same points are large, so that the new polynomial has distinct roots $\alpha_1, \dots, \alpha_t$ which are respectively close to $\xi_1, \dots, \xi_t$, as required. The precise estimates needed for this are established in §4.

Let $E_n$ denote the $K$-vector space of polynomials of $K[T]$ of degree at most $n$, and let $g\colon E_n \times E_n^* \to K$ be a non-degenerate $K$-bilinear form, where $E_n^*$ is any fixed $K$-vector space with the same dimension $n+1$ as $E_n$. In order to produce families of $n+1$ linearly independent polynomials in $E_n$ as wanted, we use adelic geometry of numbers, asking that the last minimum of certain adelic convex bodies attached to $E_n$ is at most one. This is equivalent to asking that slight dilations of their dual convex bodies, attached to $E_n^*$, have their first minimum greater than one or, more simply, that they contains no non-zero element of $E_n^*$. Precise definitions and relevant results are given in §3.

For the approximation results, the choice of the non-degenerate bilinear form is irrelevant, and we use a standard bilinear form $\varphi\colon E_n \times K^{n+1} \to K$. Then, there is no useful interpretation for the elements of the dual convex bodies in $K^{n+1}$. However, when the points $\xi_1, \dots, \xi_t$ form an arithmetic progression with non-zero difference in $K$ or a geometric progression with non-torsion ratio in $K^\times$, we construct in §5 special "translation-invariant" bilinear forms $g\colon E_n \times E_n \to K$ for which the dual convex bodies have the same form as the original ones except that the points $\xi_1, \dots, \xi_t$ are replaced by the next $n+1-t$ points $\xi_{t+1}, \dots, \xi_{n+1}$ in the corresponding arithmetic or geometric progression. Showing that the dual convex bodies contain no non-zero element of $E_n$ for arbitrarily large values of the parameters then translates into a version of Gel'fond's criterion in degree $n$ which is Theorem 2.3 above. The reader not interested in this criterion may skip §5, while the reader only interested in it may skip §4. The difficulty of finding appropriate bilinear form for other choices of points appears to be an obstacle for extending the criterion to more general situations.

In §6, we apply the above mentioned principles to reduce the proof of our main results to the statement that a certain sequence of adelic convex bodies indexed by a real parameter $X \geq 1$ contains no non-zero element of $K^{n+1}$ for arbitrarily large values of $X$. The proof of the latter proceeds by contradiction. It is done by extending the arguments of [14, §§6–8] to the present more general context. The goal, like in [6], is to replace the sequence of convex bodies by a sequence of polynomials taking small values at one fixed point and then to derive a contradiction using an appropriate version of Gel'fond's criterion. Here we use a version of Gel'fond's criterion for algebraic curves extending both [14, Thm. 4.2] and [6, Thm. 2b], which we prove in an appendix. We apply it to the point $(\xi_1, \dots, \xi_t)$ and to an algebraic curve containing that point. The polynomials that we need are constructed in §7, and estimates for their degree and height are obtained indirectly using auxiliary polynomials in §8. The proof is completed in §9.

**Additional notation.** In the sequel, we use the same notions of heights as in [14, §2].

(i) At each place $v \in \mathcal{M}$, we define the *norm* of an element $\mathbf{x} = (x_1, \dots, x_n)$ of $K_v^n$ as its maximum norm $\|\mathbf{x}\|_v = \max_{1 \leq i \leq n} |x_i|_v$. Accordingly, we define the *height* of a point $\mathbf{x} \in K^n$ by $\mathrm{H}(\mathbf{x}) = \prod_{v \in \mathcal{M}} \|\mathbf{x}\|_v$.

(ii) We denote by $E_n$ the vector space over $K$ consisting of all polynomials $P$ of $K[T]$ with degree at most $n$. We define the *height* $\mathrm{H}(P)$ of a polynomial $P \in E_n$ as the height of its vector of coefficients in $K^{n+1}$. Using the notation introduced just before the statement of Theorem 2.3, this is also given by $\mathrm{H}(P) = \prod_{v \in \mathcal{M}} \|P\|_v$. In view of our notion of height of algebraic numbers, we also note that, if $\alpha \in \bar{K}$ has degree at most $n$ over $K$ and if $P \in E_n$ is the irreducible polynomial of $\alpha$ in $K[T]$, then we have $\mathrm{H}(\alpha) \leq c\mathrm{H}(P)^d$ with a constant $c > 0$ depending only on $n$ and $d$ (see [14, §2]).

(iii) Given a place $v \in \mathcal{M}$, an integer $m$ with $1 \leq m \leq n$, and an $m \times n$ matrix $M$ with coefficients in $K_v$, we define $\|M\|_v$ as the largest absolute value of the minors of order $m$ of $M$. When $M$ has coefficients in $K$, we define its *height* by $\mathrm{H}(M) = \prod_{v \in \mathcal{M}} \|M\|_v$.

(iv) The *height* of a subspace $V$ of $E_n$ of dimension $m \geq 1$ is defined as the height of any $m \times (n+1)$ matrix $M$ whose rows are the vectors of coefficients of a basis of $V$ over $K$. In particular, if $P$ is a non-zero element of $E_{n-m+1}$ for some integer $m \geq 1$, and if $V = P \cdot E_{m-1}$ is the subspace of $E_n$ consisting of all products $PQ$ with $Q \in E_{m-1}$, then Proposition 5.2 of [14] gives $c^{-1}\mathrm{H}(P)^m \leq \mathrm{H}(V) \leq c\mathrm{H}(P)^m$ with a constant $c > 0$ which depends only on $n$.

## 3. Adelic geometry of numbers

Let $E$ be a vector space over $K$ of finite dimension $m \geq 1$ (in practice, this will be the space $E_n$ of polynomials of $K[T]$ of degree at most $n$). For each place $v$ of $K$, we put $E_v = K_v \otimes_K E$. We also put $E_{\mathbb{A}} = K_{\mathbb{A}} \otimes_K E$, where $K_{\mathbb{A}}$ denotes the adele ring of $K$ (see §14 of [4]). We define on these spaces the natural topology for which any $K$-linear isomorphism $\psi \colon E \to K^m$ extends by linearity to a $K_v$-linear homeomorphism $\psi_v \colon E_v \to K_v^m$ for each

$v \in \mathcal{M}$, and to a $K_{\mathbb{A}}$-linear homeomorphism $\psi_{\mathbb{A}} \colon E_{\mathbb{A}} \to K_{\mathbb{A}}^m$. We identify $E$ as a sub-$K$-vector space of each of these spaces under the natural embeddings $E \hookrightarrow E_v$ and $E \hookrightarrow E_{\mathbb{A}}$ mapping a point $P$ of $E$ to $1 \otimes P$. Then, $E_{\mathbb{A}}$ is a locally compact abelian group and $E$ is a discrete subgroup of $E_{\mathbb{A}}$ with compact quotient $E_{\mathbb{A}}/E$. We equip $E_{\mathbb{A}}$ with the unique Haar measure, denoted Vol, for which the quotient $E_{\mathbb{A}}/E$ has measure 1.

As $K_{\mathbb{A}}$ is a topological subring of $\prod_{v \in \mathcal{M}} K_v$, we may also view $E_{\mathbb{A}}$ as a topological subspace of $\prod_{v \in \mathcal{M}} E_v$. We define a *convex body* of $E_{\mathbb{A}}$ (or simply of $E$) to be a compact neighborhood of 0 in $E_{\mathbb{A}}$ of the form $\mathcal{C} = \prod_{v \in \mathcal{M}} \mathcal{C}_v$ where, for each $v \in \mathcal{M}$, each $P, Q \in \mathcal{C}_v$ and each $a, b \in K_v$, we have $aP + bQ \in \mathcal{C}_v$ provided that $|a|_v + |b|_v \leq 1$ if $v \in \mathcal{M}_\infty$, or that $\max\{|a|_v, |b|_v\} \leq 1$ if $v \notin \mathcal{M}_\infty$. Given a $K$-linear isomorphism $\psi \colon E \to K^m$, this is equivalent to asking that $\psi_{\mathbb{A}}(\mathcal{C})$ is a product $\prod_{v \in \mathcal{M}} \mathcal{K}_v$ where $\mathcal{K}_v$ is, in the usual sense, a convex body of $K_v^m$ when $v$ is Archimedean, and a free sub-$\mathcal{O}_v$-module of $K_v^m$ of rank $m$ otherwise, with $\mathcal{K}_v = \mathcal{O}_v^m$ for all but finitely many ultrametric places $v$, where $\mathcal{O}_v$ denotes the ring of integers of $K_v$.

For a convex body $\mathcal{C} = \prod_{v \in \mathcal{M}} \mathcal{C}_v$ of $E$ and an idele $\rho = (\rho_v)_{v \in \mathcal{M}} \in K_{\mathbb{A}}^\times$ of $K$, we denote by $\rho\mathcal{C}$ the product $\prod_{v \in \mathcal{M}} \rho_v \mathcal{C}_v$. This is again a convex body of $E$. For a positive real number $\lambda$, we also define $\lambda\mathcal{C}$ to be the product $\prod_{v \in \mathcal{M}} \rho_v \mathcal{C}_v$ where $\rho_v = 1$ for each $v \in \mathcal{M} \setminus \mathcal{M}_\infty$ and where $\rho_v = \lambda$ for each $v \in \mathcal{M}_\infty$ (using the natural topological embedding of $\mathbb{R}$ into $K_v$ extending the inclusion of $\mathbb{Q}$ into $K$). Finally, for $i = 1, \ldots, m$, we define the $i$-th minimum of $\mathcal{C}$, denoted $\lambda_i(\mathcal{C})$, to be the smallest real number $\lambda > 0$ such that $\lambda\mathcal{C}$ contains at least $i$ linearly independent elements of $E$ over $K$.

It follows from the above that, if $E'$ is another vector space of dimension $m$ over $K$ and if $\varphi \colon E \to E'$ is a $K$-linear isomorphism, then the $K_{\mathbb{A}}$-linear map $\varphi_{\mathbb{A}} \colon E_{\mathbb{A}} \to E'_{\mathbb{A}}$ which extends $\varphi$ maps any convex body $\mathcal{C}$ of $E$ to a convex body $\mathcal{C}'$ of $E'$ with the same volume and the same successive minima.

In this context, the adelic version of Minkowski's second convex body theorem proved independently by McFeat [10] and by Bombieri and Vaaler [3, Thm. 3] reads as follow.

**Proposition 3.1.** *Let $\mathcal{C}$ be an adelic convex body of $E$ and let $\lambda_1, \ldots, \lambda_m$ denote its successive minima. Then, we have $(\lambda_1 \cdots \lambda_m)^d \mathrm{Vol}(\mathcal{C}) \leq 2^{md}$.*

We will also need the following version of Mahler's duality principle.

**Proposition 3.2.** *Let $E^*$ be another vector space over $K$ of dimension $m$, let $g \colon E \times E^* \to K$ be a non-degenerate $K$-bilinear form, and let $\mathcal{C}$ be an adelic convex body of $E$. For each place $v$ of $K$, define*

$$\mathcal{C}_v^g = \{y \in E_v^* \,;\, |g_v(x, y)|_v \leq 1 \text{ for each } x \in \mathcal{C}_v\},$$

*where $g_v \colon E_v \times E_v^* \to K_v$ denotes the $K_v$-bilinear form which extends $g$. Then, $\mathcal{C}^g = \prod_{v \in \mathcal{M}} \mathcal{C}_v^g$ is an adelic convex body of $E^*$. Moreover, if $\lambda_1, \ldots, \lambda_m$ denote the successive minima of $\mathcal{C}$ and $\lambda_1^g, \ldots, \lambda_m^g$ those of $\mathcal{C}^g$, then we have $1 \leq \lambda_i \lambda_{m+1-i}^g \leq c_1$ for $i = 1, \ldots, m$ with a constant $c_1 \geq 1$ depending only on $K$ and $m$.*

We refer to $\mathcal{C}^g$ as the *dual* of $\mathcal{C}$ with respect to $g$.

*Proof.* This follows from Lemma 3.1 (ii) and Theorem 3.7 of [2], in the case where $E = E^* = K^m$ and where $g$ is the usual bilinear form $\theta\colon K^m \times K^m \to K$ given by $\theta(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^m x_i y_i$ for each $\mathbf{x} = (x_1, \dots, x_m)$ and each $\mathbf{y} = (y_1, \dots, y_m)$ in $K^m$ (see also Theorem 1 of [5] for the case $K = \mathbb{Q}$). To deduce the general case, choose $K$-linear isomorphisms $\psi\colon E \to K^m$ and $\psi^*\colon E^* \to K^m$ satisfying $g(P, Q) = \theta(\psi(P), \psi^*(Q))$ for each $(P, Q) \in E \times E^*$. Put $\mathcal{K} = \prod_{v\in\mathcal{M}} \psi_v(\mathcal{C}_v)$ and $\mathcal{K}^\theta = \prod_{v\in\mathcal{M}} \psi_v^*(\mathcal{C}_v^*)$. Then, $\mathcal{K}^\theta$ is the dual of $\mathcal{K}$ with respect to $\theta$ and so, by Lemma 3.1 of [2], $\mathcal{K}^\theta$ is a convex body of $K^m$ which in turn implies that $\mathcal{C}^g$ is a convex body of $E^*$. Moreover, the successive minima of $\mathcal{K}$ and $\mathcal{K}^\theta$ being respectively the same as those of $\mathcal{C}$ and $\mathcal{C}^g$, Theorem 3.7 of [2] gives $1 \le \lambda_i \lambda_{m+1-i}^g \le c_1$ for $i = 1, \dots, m$ with an explicit constant $c_1 = c_1(K, m)$. □

*Remark.* With the notation of Proposition 3.2, if a point $P \in E$ belongs to the interior of $\mathcal{C}$ and if $Q \in E^*$ belongs to $\mathcal{C}^g$, then the element $g(P, Q)$ of $K$ satisfies $|g(P, Q)|_v < 1$ for each $v \in \mathcal{M}_\infty$ and $|g(P, Q)|_v \le 1$ for each $v \in \mathcal{M} \setminus \mathcal{M}_\infty$. This gives $\prod_{v\in\mathcal{M}} |g(P, Q)|_v < 1$ and so $g(P, Q) = 0$ by virtue of the product formula.

We also recall the statement of the strong approximation theorem (see [9, Thm. 3, p. 440] or [4, §15]).

**Lemma 3.3.** *There exists a constant $c_2 > 0$ depending only on $K$ with the following property. Let $\mathcal{S}$ be a finite set of places of $K$ and, for each $v \in \mathcal{S}$, let $\theta_v$ be an element of $K_v$ and let $\epsilon_v$ be a positive real number. Assume that $\prod_{v\in\mathcal{S}} \epsilon_v \ge c_2$. Then, there exists an element $a$ of $K$ satisfying $|a - \theta_v|_v \le \epsilon_v$ for each $v \in \mathcal{S}$, and $|a|_v \le 1$ for each $v \in \mathcal{M} \setminus \mathcal{S}$.*

As a first application, we note the following simple consequence.

**Proposition 3.4.** *Let $\mathcal{C} = \prod_{v\in\mathcal{M}} \mathcal{C}_v$ be an adelic convex body of $E$, and let $\rho = (\rho_v)_{v\in\mathcal{M}} \in K_{\mathbb{A}}^\times$ be an idele of $K$. Define the* content *of $\rho$ to be $c(\rho) = \prod_{v\in\mathcal{M}} |\rho_v|_v$. Then, for $i = 1, \dots, m$, we have $c_2^{-1}\lambda_i(\mathcal{C}) \le c(\rho)\lambda_i(\rho\mathcal{C}) \le c_2\lambda_i(\mathcal{C})$.*

*Proof.* Fix an index $i$ with $1 \le i \le m$ and put $\lambda = \lambda_i(\mathcal{C})$, so that $\lambda\mathcal{C}$ contains $i$ linearly independent elements $P_1, \dots, P_i$ of $E$. Choose also a real number $c$ with $c > c_2 c(\rho)^{-1}$, and an ultrametric place $u$ of $K$ with $|\rho_u|_u = 1$. Then, by Lemma 3.3, there exists an element $a$ of $K$ satisfying $|a|_v \le c^{d_v/d}|\rho_v|_v$ for each $v \in \mathcal{M}_\infty$, $|a|_v \le |\rho_v|_v$ for each $v \notin \mathcal{M}_\infty \cup \{u\}$, and also $|a-1|_u < 1$. The last condition $|a-1|_u < 1$ implies that $a$ is non-zero and gives $|a|_u \le |\rho_u|_u$. Then $aP_1, \dots, aP_i$ are linearly independent elements of $E$ which belong to $a\lambda\mathcal{C}_v \subseteq c\lambda\rho_v\mathcal{C}_v$ for each $v \in \mathcal{M}_\infty$ and belong to $a\mathcal{C}_v \subseteq \rho_v\mathcal{C}_v$ for each $v \notin \mathcal{M}_\infty$, showing that $\lambda_i(\rho\mathcal{C}) \le c\lambda$. By virtue of the choice of $c$, this proves that $c(\rho)\lambda_i(\rho\mathcal{C}) \le c_2\lambda_i(\mathcal{C})$. The lower bound for $c(\rho)\lambda_i(\rho\mathcal{C})$ follows from this inequality by applying it to the pair $\rho\mathcal{C}$ and $\rho^{-1}$ instead of $\mathcal{C}$ and $\rho$, upon noting that $c(\rho^{-1}) = c(\rho)^{-1}$. □

The last proposition formalizes the construction of Davenport and Schmidt in [6, §2].

**Proposition 3.5.** *Let $\mathcal{C} = \prod_{v\in\mathcal{M}} \mathcal{C}_v$ be an adelic convex body of $E$, and let $\mathcal{S}$ be a finite set of places of $K$. For each $v \in \mathcal{S}$, choose $P_v \in E_v$ and $\rho_v \in K_v$ satisfying $\prod_{v\in\mathcal{S}} |\rho_v|_v \geq c_2 m\lambda_m(\mathcal{C})$. Then, there exists an element $P$ of $E$, satisfying $P - P_v \in \rho_v\mathcal{C}_v$ for each $v \in \mathcal{S}$, and $P \in \mathcal{C}_v$ for each $v \in \mathcal{M} \setminus \mathcal{S}$.*

*Proof.* Defining $P_v = 0$ and $\rho_v = 1$ for each Archimedean place $v$ of $K$ not in $\mathcal{S}$, we may assume, without loss of generality, that $\mathcal{M}_\infty \subseteq \mathcal{S}$. Put $\lambda = \lambda_m(\mathcal{C})$. By definition, the convex body $\lambda\mathcal{C}$ contains a basis $\{P_1, \dots, P_m\}$ of $E$ over $K$. For each place $v \in \mathcal{S}$, this basis is also a basis of $E_v$ over $K_v$ and so we can write

$$P_v = \theta_{1,v}P_1 + \cdots + \theta_{m,v}P_m$$

with $\theta_{1,v}, \dots \theta_{m,v} \in K_v$. Define $\epsilon_v = |\rho_v|_v$ for each $v \in \mathcal{S} \setminus \mathcal{M}_\infty$ and $\epsilon_v = (m\lambda)^{-d_v/d}|\rho_v|_v$ for each $v \in \mathcal{M}_\infty$. Since we have $\prod_{v\in\mathcal{S}} \epsilon_v \geq c_2$, Lemma 3.3 provides, for $i = 1, \dots, m$, an element $a_i$ of $K$ satisfying $|a_i|_v \leq 1$ for any $v \in \mathcal{M} \setminus \mathcal{S}$, and $|a_i - \theta_{i,v}|_v \leq \epsilon_v$ for any $v \in \mathcal{S}$. We claim that the polynomial $P = a_1P_1 + \cdots + a_mP_m$ has all the required properties. First of all, for each $v \in \mathcal{M}_\infty$ and for $i = 1, \dots, m$, we have $|a_i - \theta_{i,v}|_v \leq |(m\lambda)^{-1}\rho_v|_v$ and $P_i \in \lambda\mathcal{C}_v$, so that all products $(a_i - \theta_{i,v})P_i$ belong to $m^{-1}\rho_v\mathcal{C}_v$ and their sum $P - P_v$ belongs to $\rho_v\mathcal{C}_v$. For each $v \in \mathcal{S} \setminus \mathcal{M}_\infty$, we have instead $|a_i - \theta_{i,v}|_v \leq |\rho_v|_v$ and $P_i \in \mathcal{C}_v$ for each $i$, so that $\rho_v\mathcal{C}_v$ contains all products $(a_i - \theta_{i,v})P_i$ and also their sum $P - P_v$. Finally, for each of the remaining ultrametric places $v \in \mathcal{M} \setminus \mathcal{S}$, we have $a_iP_i \in a_i\mathcal{C}_v \subseteq \mathcal{C}_v$ for each $i$, and so $P \in \mathcal{C}_v$. □

## 4. Approximation

Let $n$ and $t$ be integers with $1 \leq t \leq n$, and let $(\xi_1, \dots, \xi_t)$ be a point of $K_w^t$. We denote by $\eta_1, \dots, \eta_s$ the distinct elements of the sequence $(\xi_1, \dots, \xi_t)$ and, for each $i = 1, \dots, s$, we denote by $m_i$ the number of times that $\eta_i$ appears in this sequence. The constants $c_3, c_4, \dots$ that appear below, as well as the implied constants in the symbols $\ll$ and $\gg$ depend only on $K$, $w$ and the above quantities.

As mentioned in §2, we denote by $E_n$ the vector space over $K$ consisting of all polynomials of $K[T]$ of degree $\leq n$. Then, for each $v \in \mathcal{M}$, the $K_v$-vector space $E_{n,v} = K_v \otimes_k E_n$ identifies itself with the space of polynomials of $K_v[T]$ of degree $\leq n$. For each pair of real numbers $X, Y \geq 1$, we define $\mathcal{C}(X, Y)$ to be the convex body of $E_n$ whose component $\mathcal{C}_v(X, Y)$ at each place $v \in \mathcal{M}$ distinct from $w$ consists of all polynomials $P$ of $E_{n,v}$ with $\|P\|_v \leq 1$, and whose component $\mathcal{C}_w(X, Y)$ at $w$ consists of all polynomials $P$ of $E_{n,w}$ with

$$\|P\|_w \leq X \quad \text{and} \quad \max_{1\leq i\leq s} \Big( \max_{0\leq j<m_i} |P^{(j)}(\eta_i)|_w \Big) \leq Y^{-1}, \tag{3}$$

where $P^{(j)}$ stands for the $j$-th derivative of $P$. Our goal in this section is to prove the following result of approximation which in a sense extends Lemma 9.1 of [14].

**Proposition 4.1.** *Let $X, Y$ be real numbers with $X, Y \geq 1$ and let $\lambda$ denote the $(n+1)$-th minimum of the convex body $\mathcal{C}(X,Y)$ of $E_n$. Then there exists an irreducible polynomial $P \in K[T]$ of degree $n$ and height at most $c_3\lambda X$ which, for $i = 1, \ldots, s$, admits at least $m_i$ roots in the closed disk of $K_w$ of radius $c_4(XY)^{-1/m_i}$ centered at $\eta_i$, without vanishing at $\eta_i$.*

*Proof.* Choose a finite place $u$ of $K$ with $u \neq w$, and a uniformizing parameter $\pi \in \mathcal{O}_u$ for $u$. Define $P_u = T + \pi$ and $\rho_u = \pi^2$. By Proposition 3.5, there is a constant $c_5 > 0$ such that, for any choice of $P_w \in E_{n,w}$ and $\rho_w \in K_w$ with $|\rho_w|_w \geq c_5\lambda$, there is a polynomial $P \in E_n$ which satisfies $P \in \mathcal{C}_v(X,Y)$ for each $v \in \mathcal{M} \setminus \{u, w\}$, and $P - P_v \in \rho_v \mathcal{C}_v(X,Y)$ for each $v \in \{u, w\}$. The condition at $u$ reads

$$\|P - (T^n + \pi)\|_u \leq |\pi|_u^2.$$

By virtue of Eisenstein's criterion, it implies that such a polynomial $P$ is irreducible over $K_u$ and so is irreducible over $K$. It also gives $\|P\|_u \leq 1$. Since, for each $v \notin \{u, w\}$, the condition $P \in \mathcal{C}_v(X,Y)$ means $\|P\|_v \leq 1$, we deduce that

$$\mathrm{H}(P) \leq \|P\|_w. \tag{4}$$

Choose $\rho_w$ to be an element of $K_w$ of smallest norm with $|\rho_w|_w \geq c_5\lambda$. Then, we have $|\rho_w|_w \ll \lambda$, and the last condition $P - P_w \in \rho_w \mathcal{C}_w(X,Y)$ leads to

$$\begin{aligned} \|P - P_w\|_w &\ll \lambda X, \\ |(P - P_w)^{(j)}(\eta_i)|_w &\ll \lambda Y^{-1} \quad (1 \leq i \leq s,\ 0 \leq j < m_i). \end{aligned} \tag{5}$$

We look for a polynomial $P_w$ of the form

$$P_w(T) = a \prod_{i=1}^{s} \prod_{j=1}^{m_i} (T - \eta_i - jz_i)$$

with $a, z_1, \ldots, z_s \in K_w \setminus \{0\}$. To choose the latter parameters, we note that there exists a constant $c_6$ with $0 < c_6 < (n!)^{-1}$ such that any polynomial $Q \in E_{n,w}$ which satisfies

$$\Big\| Q(T) - \prod_{j=1}^{\ell} (T - j) \Big\|_w \leq c_6$$

for some integer $\ell$ with $1 \leq \ell \leq n$ admits at least $\ell$ distinct roots of norm at most $|\ell|_w + 1$ in $K_w$. Putting

$$\sigma_i = a z_i^{m_i} \prod_{k \neq i} (\eta_i - \eta_k)^{m_k} \quad (1 \leq i \leq s),$$

where the product extends to all integers $k = 1, \ldots, s$ with $k \neq i$, we find

$$\sigma_i^{-1} P_w(z_i T + \eta_i) - \prod_{j=1}^{m_i} (T - j) = \Big( \prod_{k \neq i} \prod_{j=1}^{m_k} \Big( 1 + \frac{z_i T - j z_k}{\eta_i - \eta_k} \Big) - 1 \Big) \prod_{j=1}^{m_i} (T - j)$$

so that

$$\Big\| \sigma_i^{-1} P_w(z_i T + \eta_i) - \prod_{j=1}^{m_i} (T - j) \Big\|_w \leq c_7 \max_{1 \leq k \leq s} |z_k|_w \tag{6}$$

for some constant $c_7 \geq 1$. We now fix $z_1, \dots, z_s \in K_w$ of maximal absolute value with

$$|z_i|_w \leq \frac{c_6}{2c_7}(XY)^{-1/m_i} \quad (1 \leq i \leq s).$$

Then the right hand side of (6) is bounded above by $c_6/2$ and using the hypotheses (5) on $P$ we find, for each $i = 1, \dots, s$,

$$\begin{aligned} \Big\|\sigma_i^{-1}P(z_iT + \eta_i) - \prod_{j=1}^{m_i}(T-j)\Big\|_w &\leq \frac{c_6}{2} + |\sigma_i|_w^{-1}\|P(z_iT+\eta_i) - P_w(z_iT+\eta_i)\|_w \\ &= \frac{c_6}{2} + |\sigma_i|_w^{-1} \max_{0\leq j\leq n}\Big|\frac{1}{j!}(P-P_w)^{(j)}(\eta_i)\Big|_w |z_i|_w^j \\ &\leq \frac{c_6}{2} + c_8\lambda|a|_w^{-1}X, \end{aligned} \tag{7}$$

with a constant $c_8 > 0$. Finally, we fix $a \in K_w$ of minimal absolute value with

$$|a|_w \geq \frac{2c_8}{c_6}\lambda X.$$

Then the left hand side of (7) is at most $c_6$ and accordingly the polynomial $P$ admits at least $m_i$ distinct roots in the ball of $K_w$ of radius $(|m_i|_w + 1)|z_i|_w$ centered at $\eta_i$. Moreover, substituting $T = 0$ in (7) provides $|\sigma_i^{-1}P(\eta_i) \pm m_i!|_w \leq c_6 < |m_i!|_w$, and so we must have $P(\eta_i) \neq 0$. The choice of $a$ also gives $\|P_w\|_w \ll \lambda X$. Combining this with (4) and (5), we deduce that $\mathrm{H}(P) \ll \lambda X$. Thus $P$ has all the required properties. □

## 5. Invariant bilinear forms

Assume that the points $\xi_1, \dots, \xi_t$ introduced in the previous section §4 come from a sequence $\xi_1, \dots, \xi_{n+1}$ of $n+1$ distinct elements of $K_w$ which is either an arithmetic progression with difference $\gamma \in K^\times$ (the additive case), or a geometric progression with ratio $\gamma \in K^\times$ satisfying $\xi_1 \neq 0$ and $\gamma^i \neq 1$ for $i = 1, \dots, 2n$ (the multiplicative case).

Then, for each pair of real numbers $X, Y \geq 1$, the convex body $\mathcal{C}(X,Y)$ of $E_n$ introduced in the previous section is the product $\prod_{v\in\mathcal{M}} \mathcal{C}_v(X,Y)$ where

$$\mathcal{C}_w(X,Y) = \{P \in E_{n,w}\,;\, \|P\|_w \leq X \text{ and } \max_{1\leq i\leq t}|P(\xi_i)|_w \leq Y^{-1}\}, \tag{8}$$

and where, for $v \neq w$, the component $\mathcal{C}_v(X,Y)$ consists of all polynomials $P$ of $E_{n,v}$ with $\|P\|_v \leq 1$. Similarly, we define another convex body $\bar{\mathcal{C}}(X,Y) = \prod_{v\in\mathcal{M}} \bar{\mathcal{C}}_v(X,Y)$ by putting

$$\bar{\mathcal{C}}_w(X,Y) = \{Q \in E_{n,w}\,;\, \|Q\|_w \leq Y \text{ and } \max_{t+1\leq i\leq n+1}|P(\xi_i)|_w \leq X^{-1}\}, \tag{9}$$

and $\bar{\mathcal{C}}_v(X,Y) = \mathcal{C}_v(X,Y)$ for every $v \neq w$. Our goal is to show that these convex bodies $\mathcal{C}(X,Y)$ and $\bar{\mathcal{C}}(X,Y)$ are essentially dual to each other with respect to the bilinear form $g$ constructed by the following proposition.

**Proposition 5.1.** *Let $\gamma \in K^\times$ be as above (with $\gamma^i \neq 1$ for $i = 1, \dots, 2n$ in the multiplicative case). For each integer $i \geq 0$, we define $\gamma_i = i\gamma$ in the additive case, and $\gamma_i = \gamma^i$ in the multiplicative case. For each $x \in K$, we also denote by $\tau_x \colon E_n \to E_n$ the linear map given by*

*$\tau_x(P(T)) = P(x+T)$ in the additive case, and by $\tau_x(P(T)) = P(xT)$ in the multiplicative case. Then, in each case, there exist elements $g_{ij}$ of $K$ for $0 \le i \le j \le n$ such that the bilinear form $g\colon E_n \times E_n \to K$ given by*

$$g(P,Q) = \sum_{0\le i\le j\le n} g_{ij} P(\gamma_i) Q(\gamma_j) \tag{10}$$

*is non-degenerate and satisfies, for any $x \in K$ and any $P, Q \in E_n$,*

$$g(\tau_x P, \tau_x Q) = \begin{cases} g(P,Q) & \text{in the additive case,} \\ x^n g(P,Q) & \text{in the multiplicative case.} \end{cases} \tag{11}$$

*Proof.* The hypothesis on $\gamma$ ensures that the points $\gamma_0, \gamma_1, \dots, \gamma_{2n}$ are all distinct. In particular, the first $n+1$ of them are distinct and so there exists a unique choice of elements $a_0, a_1, \dots, a_{n+1}$ of $K$ with $a_{n+1} = 1$ such that

$$\sum_{i=0}^{n+1} a_i P(\gamma_i) = 0 \tag{12}$$

for any $P \in E_n$.

Fix temporarily $P \in E_n$. In the additive case, we put $\rho = 1$ and $\tilde{P}(T) = P((n+1)\gamma - T)$. In the multiplicative case, we put $\rho = \gamma^n$ and $\tilde{P}(T) = T^n P(\gamma^{n+1} T^{-1})$. Then $\tilde{P}$ belongs to $E_n$ and the formula (12) applied to $\tilde{P}$ becomes

$$\sum_{i=0}^{n+1} \rho^i a_i P(\gamma_{n+1-i}) = 0.$$

From this we deduce that

$$\sum_{i=0}^{n+1} \rho^{n+1-i} a_{n+1-i} P(\gamma_i) = 0 \tag{13}$$

for any $P \in E_n$ and so, although we will not need it, we get $\rho^{n+1-i} a_{n+1-i} = a_0 a_i$ for $i = 0, 1, \dots, n+1$.

Let $g\colon E_n \times E_n \to K$ be the bilinear form given by (10) for the choice of coefficients

$$g_{ij} = \rho^{n-j} a_{n+1+i-j} \quad (0 \le i \le j \le n). \tag{14}$$

Since $g_{ii} \neq 0$ for $i = 0, 1, \dots, n$, this bilinear form is non-degenerate. Moreover, for any pair of polynomials $P, Q \in E_n$, we find, using (12), (13) and (14),

$$\begin{aligned} g(\tau_\gamma P, \tau_\gamma Q) &= \sum_{0\le i\le j\le n-1} g_{ij} P(\gamma_{i+1}) Q(\gamma_{j+1}) + \sum_{0\le i\le n} a_{i+1} P(\gamma_{i+1}) Q(\gamma_{n+1}) \\ &= \sum_{1\le i\le j\le n} \rho g_{ij} P(\gamma_i) Q(\gamma_j) - a_0 P(\gamma_0) Q(\gamma_{n+1}) \\ &= \rho g(P,Q) - P(\gamma_0) \sum_{0\le j\le n+1} \rho^{n+1-j} a_{n+1-j} Q(\gamma_j) \\ &= \rho g(P,Q). \end{aligned}$$

By recurrence, we deduce that the formula (11) holds for $x = \gamma_i$ with $i = 0, 1, \dots, 2n$. Since these $2n+1$ numbers are distinct, and since $g(\tau_x P, \tau_x Q)$ is, for fixed $P$ and $Q$, a polynomial in $x$ of degree at most $2n$, the formula must therefore hold for any $x \in K$. □

*Remark* 1. In the additive (resp. multiplicative) case, the property (11) expresses an invariance of the bilinear form $g$ under the additive (resp. multiplicative) group of $K$. One may wonder if similar invariant "triangular" forms can be defined for elliptic curves defined over $K$. In the present context, it is interesting to note that the bilinear form $g\colon E_n \times E_n \to K$ defined in [14, Lemma 3.3] in terms of the derivatives of the polynomials at 0 possesses both invariance properties stated in (11).

*Remark* 2. In the notation of the proof, one finds for $i = 0, 1, \dots, n$ that $a_i = -P_i(\gamma_{n+1})$ where $P_i$ denotes the element of $E_n$ which takes the value 1 at $\gamma_i$ and vanishes at all other points $\gamma_j$ with $0 \le j \le n$ and $j \ne i$, and therefore

$$a_i = -\prod_{j \ne i} \frac{\gamma_{n+1} - \gamma_j}{\gamma_i - \gamma_j}$$

where the product extends over all indices $j$ with $0 \le j \le n$ with $j \ne i$. In particular, in the additive case, we find that $a_i = (-1)^{n+1-i}\binom{n+1}{i}$ is independent of $\gamma$. We will not need these explicit formulas here.

Coming back to the adelic convex bodies $\mathcal{C}(X,Y)$ and $\bar{\mathcal{C}}(X,Y)$, we can now state the result which was alluded to at the beginning of the section.

**Proposition 5.2.** *There exist ideles $\alpha, \beta \in K_{\mathbb{A}}^{\times}$ such that, for any choice of real numbers $X, Y \ge 1$, we have*

$$\alpha\bar{\mathcal{C}}(X,Y) \subseteq \mathcal{C}^g(X,Y) \subseteq \beta\bar{\mathcal{C}}(X,Y), \tag{15}$$

*where $\mathcal{C}^g(X,Y)$ denotes the dual of $\mathcal{C}(X,Y)$ with respect to the bilinear form $g$ given by Proposition 5.1.*

*Proof.* Let $g_w\colon E_{n,w} \times E_{n,w} \to K_w$ denote the $K_w$-bilinear form which extends $g$. The invariance property (11) of $g$ extends by continuity to $g_w$ for each $x \in K_w$, with the map $\tau_x\colon E_{n,w} \to E_{n,w}$ defined by the same formula as in Proposition 5.1. Taking $x = \xi_1$, this gives

$$g_w(P,Q) = \sum_{0 \le i \le j \le n} \rho g_{ij} P(\xi_{i+1}) Q(\xi_{j+1}) \tag{16}$$

for any $P, Q \in E_{n,w}$, with $\rho = 1$ in the additive case and $\rho = \xi_1^{-n}$ in the multiplicative case. From this and the definitions (8) and (9), we deduce that $|g_w(P,Q)|_w \le c$ for each $P \in \mathcal{C}_w(X,Y)$ and each $Q \in \bar{\mathcal{C}}_w(X,Y)$, with a constant $c > 0$ that is independent of $X$ and $Y$. Choosing $\alpha_w \in K_w^{\times}$ with $|\alpha_w|_w \le 1/c$ then gives $\alpha_w \bar{\mathcal{C}}_w(X,Y) \subseteq \mathcal{C}_w^g(X,Y)$. Conversely, since $\xi_1, \dots, \xi_{n+1}$ are distinct, there exist, for each $i = 1, \dots, n+1$, a unique polynomial $P_i \in E_{n,w}$

which vanishes at each point $\xi_j$ with $j \neq i$ and satisfies $P_i(\xi_i) = Y^{-1}$ if $i \leq t$, and $P_i(\xi_i) = X$ if $i > t$. The polynomials $P_1, \dots, P_{n+1}$ so constructed belong to $\theta\mathcal{C}_w(X,Y)$ for some constant $\theta \in K_w^\times$. Then, any $Q \in \mathcal{C}_w^g(X,Y)$ satisfies $|g_w(\theta^{-1}P_i, Q)|_w \leq 1$ for $i = 1, \dots, n+1$ which, in view of (16), translates into

$$\left| \sum_{j=i}^{n} \rho g_{ij} \theta^{-1} Q(\xi_{j+1}) \right|_w \leq \begin{cases} Y & \text{for } i = 0, \dots, t-1, \\ X^{-1} & \text{for } i = t, \dots, n. \end{cases}$$

As $g_{ii} \neq 0$ for $i = 0, \dots, n$, this implies that $\mathcal{C}_w^g(X,Y)$ is contained in $\beta_w \bar{\mathcal{C}}_w(X,Y)$ for a constant $\beta_w \in K_w^\times$. For the remaining places $v \neq w$ of $K$, the components of $\mathcal{C}(X,Y)$ and $\bar{\mathcal{C}}(X,Y)$ at $v$ are independent of $X$ and $Y$, and thus we also have

$$\alpha_v \bar{\mathcal{C}}_v(X,Y) \subseteq \mathcal{C}_v^g(X,Y) \subseteq \beta_v \bar{\mathcal{C}}_v(X,Y)$$

for some $\alpha_v, \beta_v \in K_v^\times$ which are independent of $X$ and $Y$ and can be taken to be 1 for all but finitely many places $v$. Then the ideles $\alpha = (\alpha_v)_{v \in \mathcal{M}}$ and $\beta = (\beta_v)_{v \in \mathcal{M}}$ have the property (15). □

Combining this result with Propositions 3.2 and 3.4, we deduce the following.

**Corollary 5.3.** *Let $\lambda_j(X,Y)$ and $\bar{\lambda}_j(X,Y)$ denote respectively the $j$-th minima of $\mathcal{C}(X,Y)$ and $\bar{\mathcal{C}}(X,Y)$. Then, the products $\lambda_j(X,Y)\bar{\lambda}_{n+2-j}(X,Y)$ with $1 \leq j \leq n+1$ are bounded above and below by positive constants which are independent of the choice of $X, Y \geq 1$.*

## 6. The main Proposition and deduction of the Theorems

Let the notation be as in §4, and let $\varphi\colon E_n \times K^{n+1} \to K$ be the non-degenerate $K$-bilinear form given by

$$\varphi(a_0 + a_1 T + \cdots + a_n T^n, (y_0, y_1, \dots, y_n)) = a_0 y_0 + a_1 y_1 + \cdots + a_n y_n.$$

In §4, we defined a convex body $\mathcal{C}(X,Y)$ for each pair of real numbers $X, Y \geq 1$. Accordingly, we denote by $\mathcal{C}^\varphi(X,Y)$ the convex body of $K^{n+1}$ which is dual to $\mathcal{C}(X,Y)$ with respect to $\varphi$. For $i = 1, \dots, n+1$, we also denote by $\lambda_i(X,Y)$ and $\lambda_i^\varphi(X,Y)$ the respective $i$-th minimum of $\mathcal{C}(X,Y)$ in $E_n$ and of $\mathcal{C}^\varphi(X,Y)$ in $K^{n+1}$. We show in this section how the theorems stated in §2 can be derived from the following proposition whose proof is postponed to the last section §9.

**Proposition 6.1.** *Assume that we are either in the situation of Theorem 2.1, in which case we define $\nu = 4Dst$, or in the situation of Theorem 2.2, in which case we define $\nu = 4t$. Then, there are arbitrarily large values of $X$ such that $\lambda_1^\varphi(X, X^{(n+2-\nu)/\nu}) > 1$.*

6.1. **Proof of Theorems 2.1 and 2.2.** Assume that we are in the situation of Theorem 2.1 or Theorem 2.2 and define $\nu$ accordingly as in Proposition 6.1. For each pair of real numbers $X, Y \geq 1$ satisfying $\lambda_1^{\varphi}(X,Y) > 1$, Proposition 3.2 gives $\lambda_{n+1}(X,Y) \ll \lambda_1^{\varphi}(X,Y)^{-1} \ll 1$ with implied constants which are independent of $X$ and $Y$, and then Proposition 4.1 shows the existence of an irreducible polynomial $P \in K[T]$ of degree $n$ and height $\ll X$ which, for $i = 1, \dots, s$, admits at least $m_i$ roots in a closed disk of $K_w$ of radius $\ll (XY)^{-1/m_i}$ centered at $\eta_i$, without vanishing at $\eta_i$. If the product $XY$ is sufficiently large, these disks are disjoint and we deduce that $P$ admits $t$ distinct roots $\alpha_1, \dots, \alpha_t$ satisfying $0 < |\xi_i - \alpha_i|_w \ll (XY)^{-1/m}$, where $m = \max\{m_1, \dots, m_s\}$. Moreover, if $\alpha$ is a root of $P$ in $\bar{K}$, then we have $\mathrm{H}(\alpha) \ll \mathrm{H}(P)^d \ll X^d$. Assume from now on that $Y = X^{(n+2-\nu)/\nu}$. Then the hypothesis gives $\lambda_1^{\varphi}(X,Y) > 1$ for arbitrary large values of $X$ and, for each such $X$, the above provides an algebraic number $\alpha = \alpha_X \in \bar{K}$ which, over $K$, has degree $n$ and admits distinct conjugates $\alpha_1, \dots, \alpha_t \in K_w$ satisfying $0 < |\xi_i - \alpha_i|_w \ll X^{-(n+2)/(m\nu)} \ll \mathrm{H}(\alpha)^{-(n+2)/(dm\nu)}$ for $i = 1, \dots, t$. The conclusion follows as, by varying $X$, we get infinitely many algebraic numbers $\alpha$.

6.2. **Proof of Theorem 2.3.** Let the notation and hypotheses be as in Theorem 2.3. For each pair of real numbers $X, Y \geq 1$, define $\bar{\mathcal{C}}(X,Y)$ as in §5 and, for $i = 1, \dots, n+1$, denote by $\bar{\lambda}_i(X,Y)$ the $i$-th minimum of $\bar{\mathcal{C}}(X,Y)$. According to Proposition 3.2 and Corollary 5.3, the products $\lambda_i^{\varphi}(X,Y)\lambda_{n+2-i}(X,Y)$ and $\bar{\lambda}_i(X,Y)\lambda_{n+2-i}(X,Y)$ are bounded below and above by positive constants which are independent of $X$ and $Y$. The same is therefore true of the ratios $\lambda_i^{\varphi}(X,Y)/\bar{\lambda}_i(X,Y)$. In particular there exists a constant $c > 0$ such that $\lambda_1^{\varphi}(X,Y) \leq c\bar{\lambda}_1(X,Y)$. Moreover, if $\rho = (\rho_v)_{v \in \mathcal{M}} \in K_{\mathbb{A}}^{\times}$ is an idele of $K$ satisfying $\rho_v = 1$ for each place $v \neq w$, then, putting $r = |\rho_w|_w$, we find $\rho\bar{\mathcal{C}}(X,Y) = \bar{\mathcal{C}}(r^{-1}X, rY)$ and accordingly Proposition 3.4 gives $\bar{\lambda}_i(r^{-1}X, rY) \leq c_2 r^{-1}\bar{\lambda}_i(X,Y)$ for $i = 1, \dots, n+1$. In particular, for a suitable choice of $r \geq 1$, we have

$$\lambda_1^{\varphi}(r^{-1}X, rY) \leq c\bar{\lambda}_1(r^{-1}X, rY) \leq \bar{\lambda}_1(X,Y), \tag{17}$$

independently of $X \geq r$ and $Y \geq 1$.

The hypotheses of Theorem 2.3 imply that, for each choice of $X$ and $Y$ with $1 \leq X \leq Y^{4t/(n+1-4t)}$ and $Y$ sufficiently large, the convex body $\bar{\mathcal{C}}(X,Y)$ contains a non-zero element of $E_n$, and so we have $\bar{\lambda}_1(X,Y) \leq 1$. By (17), this gives $\lambda_1^{\varphi}(r^{-1}X, rY) \leq 1$ and thus $\mathcal{C}^{\varphi}(r^{-1}X, rY)$ contains a non-zero element of $K^{n+1}$ for such choices of $X$ and $Y$. In particular, we deduce that $\mathcal{C}^{\varphi}(X, X^{(n+2-4t)/(4t)})$ contains a non-zero element of $K^{n+1}$ for each sufficiently large value of $X$. By Proposition 6.1, this means that the given points $\xi_1, \dots, \xi_{n+1}$ do not satisfy all conditions of Theorem 2.2. Thus $\xi_1$ must be algebraic over $K$ of degree less than $n/t$. Then, all of $\xi_1, \dots, \xi_{n+1}$ are algebraic over $K$ of degree less than $n/t$, by virtue of the recurrence relation which links these numbers.

## 7. Construction of a polynomial

From this point on, the objective is to prove Proposition 6.1. In this section, we fix a choice of real numbers $X, Y \geq 1$ and assume that the convex body $\mathcal{C}^{\varphi}(X,Y)$ introduced in §6 contains a non-zero point $\mathbf{y} = (y_0, y_1, \dots, y_n)$ of $K^{n+1}$. We will derive several consequences from this assumption. Again, the constants $c_9, c_{10}, \dots$ that appear below, as well as implied constants in the symbols $\ll$ and $\gg$, depend only on $K$, $n$, $w$ and the points $\xi_1, \dots, \xi_t$.

For each integer $\ell = 0, 1, \dots, n$, we denote by $B_\ell \colon E_\ell \times E_{n-\ell} \to K$ the $K$-bilinear form given by

$$B_\ell(F,G) = \varphi(FG, \mathbf{y})$$

and we define $M_\ell$ to be the matrix of $B_\ell$ with respect to the bases $\{1, T, \dots, T^\ell\}$ of $E_\ell$ and $\{1, T, \dots, T^{n-\ell}\}$ of $E_{n-\ell}$. Thus, $M_\ell$ is the matrix of size $(\ell+1) \times (n-\ell+1)$ whose element of the $i$-th row and $j$-th column is

$$B_\ell(T^{i-1}, T^{j-1}) = \varphi(T^{i+j-2}, \mathbf{y}) = y_{i+j-2}$$

for $i = 1, \dots, \ell+1$ and $j = 1, \dots, n-\ell+1$.

Our first goal is to establish an upper bound for the height $\mathrm{H}(M_\ell)$ of $M_\ell$ when $\ell \leq n/2$, a condition which ensures that $M_\ell$ has no more rows than columns (see §2 for the definition of the height). To this end, we extend $B_\ell$ to a $K_w$-bilinear form $B_{\ell,w} \colon E_{\ell,w} \times E_{n-\ell,w} \to K_w$ and we define $N_\ell$ to be the matrix of $B_{\ell,w}$ with respect to the basis $\{1, T, \dots, T^\ell\}$ of $E_{\ell,w}$ and the basis $\{R_0, R_1, \dots, R_{n-\ell}\}$ of $E_{n-\ell,w}$ where

$$R_0(T) = 1 \quad \text{and} \quad R_j(T) = (T-\xi_1)(T-\xi_2)\cdots(T-\xi_j) \quad \text{for } j = 1, \dots, n, \tag{18}$$

extending for convenience the definition of $\xi_k$ for $k = t+1, \dots, n$ by putting

$$\xi_{t+1} = \cdots = \xi_n = 0. \tag{19}$$

**Lemma 7.1.** *Let $\ell$ be an integer with $0 \leq \ell \leq n/2$, and let $\mathbf{z}_j$ denote the $j$-th column of $N_\ell$ for $j = 1, \dots, n-\ell+1$. Then, there are constants $c_9, c_{10}, c_{11} \geq 1$ such that*

(i) $\|\mathbf{z}_j\|_w \leq c_9 Y$ *for* $1 \leq j \leq t$ *and* $\|\mathbf{z}_j\|_w \leq c_9 X^{-1}$ *for* $t+1 \leq j \leq n-\ell+1$,
(ii) $\mathrm{H}(M_\ell) \leq c_{10} \|N_\ell\|_w$,
(iii) $\mathrm{H}(M_\ell) \leq c_{11} Y^t X^{-(\ell+1-t)}$.

*Proof.* Fix an index $j$ with $1 \leq j \leq n-\ell+1$. By definition, we have

$$\|\mathbf{z}_j\|_w = \max_{0 \leq i \leq \ell} |B_{\ell,w}(T^i, R_{j-1}(T))|_w = \max_{0 \leq i \leq \ell} |\varphi_w(T^i R_{j-1}(T), \mathbf{y})|_w \leq |\rho|_w^{-1}$$

for any non-zero element $\rho$ of $K_w$ such that $\rho T^i R_{j-1}(T) \in \mathcal{C}_w(X,Y)$ for $i = 0, \dots, \ell$. As $R_{j-1}(T)$ has bounded norm and as it is divisible by $(T-\xi_1)\cdots(T-\xi_t)$ when $j > t$, there exists a constant $c > 0$ such that any choice of $\rho$ with $0 < |\rho|_w \leq cY^{-1}$ will do when $1 \leq j \leq t$ and such that any choice of $\rho$ with $0 < |\rho|_w \leq cX$ will do when $t+1 \leq j \leq n-\ell+1$. The inequalities (i) follow.

Now, fix a place $v$ of $K$ with $v \neq w$. Then, we have $|\varphi_v(Q, \mathbf{y})|_v \leq 1$ for any polynomial $Q \in E_{n,v}$ with $\|Q\|_v \leq 1$. This implies that $\|\mathbf{y}\|_v \leq 1$ and therefore that

$$\|M_\ell\|_v \leq \max\{1, |(\ell+1)!|_v\}.$$

Using the inequalities (i), we also find

$$\|N_\ell\|_w \leq \max\{1, |(\ell+1)!|_w\} c_9^{\ell+1} Y^t X^{-(\ell+1-t)}$$

(this holds even when $\ell + 1 < t$). Since $M_\ell = N_\ell V$ for some matrix $V \in \mathrm{GL}_{n-\ell+1}(K_w)$ with coefficients depending only on $\xi_1, \dots, \xi_t$, $\ell$ and $n$, we also have $\|M_\ell\|_w \leq c' \|N_\ell\|_w$ for some constant $c' > 0$. Together with the previous inequalities this proves (ii) with $c_{10} = n! c'$ and (iii) with $c_{11} = n! c' c_9^n$. □

To state the next result, we denote by $V_\ell$ the right kernel of $B_\ell$ :

$$V_\ell = \{G \in E_{n-\ell}\,;\, \varphi(FG, \mathbf{y}) = 0 \text{ for all } F \in E_\ell\}, \quad (0 \leq \ell \leq n). \tag{20}$$

**Lemma 7.2.** *Suppose that we have $c_{11} Y^t < X^{k+1-t}$ for some integer $k$ with $t \leq k \leq n/2$. Then there exists an integer $h$ with $1 \leq h \leq k$ and a non-zero polynomial $P \in V_{n-h}$ which divides any element of $V_{k-1}$ and satisfies*

$$\deg(P) \leq h \quad \textit{and} \quad \mathrm{H}(P)^{n-2h+2} \leq c_{12} \mathrm{H}(M_{h-1})$$

*with a constant $c_{12} > 0$ depending only on $n$.*

*Proof.* By Lemma 7.1 (iii), the condition $c_{11} Y^t < X^{k+1-t}$ implies that $\mathrm{H}(M_k) < 1$ and so $\mathrm{H}(M_k) = 0$. Thus, $M_k$ has rank at most $k$. Since $M_0$ has rank 1, we deduce that there exists an integer $h$ with $1 \leq h \leq k$ such that $\mathrm{rank}(M_{h-1}) = h$ and $\mathrm{rank}(M_h) \leq h$. We now argue as in Lemmas 6.3 and 6.4 of [14]. Since $\mathrm{rank}(M_h) \leq h$, the left kernel of $B_h$ which is $V_{n-h}$ contains a non-zero polynomial $P$. Then we have $\deg(P) \leq h$ and $V_{h-1}$ contains the set $P \cdot E_{n-2h+1}$ of all products $PQ$ with $Q \in E_{n-2h+1}$. Since the dimension of $V_{h-1}$ is $(n-h+2) - \mathrm{rank}(M_{h-1}) = n-2h+2$ and since $P \cdot E_{n-2h+1}$ is a vector space over $K$ of the same dimension, we conclude that $V_{h-1} = P \cdot E_{n-2h+1}$. This equality has two consequences. First of all, since $V_{k-1}$ is a subspace of $V_{h-1}$, the polynomial $P$ divides all elements of $V_{k-1}$. Secondly, since $\mathrm{H}(M_{h-1})$ is, by a well-known duality principle, equal to the Schmidt height $\mathrm{H}(V_{h-1})$ of $V_{h-1}$, Proposition 5.2 of [14] shows that $\mathrm{H}(P)^{n-2h+2} \leq c_{12} \mathrm{H}(M_{h-1})$ with a constant $c_{12} > 0$ depending only on $n$ (see also §2). □

We conclude this section by showing the following additional property for the polynomial $P$ constructed in Lemma 7.2:

**Lemma 7.3.** *Let the notation and the hypotheses be as in Lemma 7.2. Assume further that $k \leq (n - t + 2)/2$. Then there exists an index $i$ with $1 \leq i \leq t$ and an irreducible factor $Q$ of $P$ such that*

$$\left( \frac{|Q(\xi_i)|_w}{\|Q\|_w} \right)^t \leq c_{13} X^{-\deg(Q)} \mathrm{H}(Q)^{-(n-2k+2)}.$$

*Proof.* Let $\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_{n-h+2}$ denote the columns of $N_{h-1}$ and, for each $j = 1, \dots, t+1$, let $N_{h-1}^{(j)}$ denote the sub-matrix of $N_{h-1}$ whose columns are $\mathbf{z}_j, \mathbf{z}_{j+1}, \dots, \mathbf{z}_{n-h+2}$. The hypothesis $k \le (n-t+2)/2$ ensures that each of these matrices has at least as many columns as rows. It also gives $h \le (n-t+2)/2$ which implies that the products $T^i R_{j-1}(T)$ with $i = 0, \dots, h-1$ and $j = 1, \dots, t$ all have degree at most $n-h$. Since $P$ belongs to $V_{n-h}$, we deduce that

$$B_{h-1,w}(T^i, R_{j-1}(T)P(T)) = B_{n-h,w}(T^i R_{j-1}(T), P(T)) = 0 \tag{21}$$

for the same values of $i$ and $j$.

Fix an index $j$ with $1 \le j \le t$. Since $\deg(P) \le h$, there exist a constant $c > 0$ and elements $a_{j,1}, \dots, a_{j,h}$ of $K_w$ of absolute value at most $c\|P\|_w$ such that, with the convention (19), we have

$$P(\xi_j) - P(T) = \sum_{\ell=1}^{h} a_{j,\ell}(T - \xi_j) \cdots (T - \xi_{j+\ell-1}).$$

Taking into account that (21) holds for $i = 0, \dots h-1$ we deduce that, for these values of $i$,

$$\begin{aligned} P(\xi_j) B_{h-1,w}(T^i, R_{j-1}(T)) &= B_{h-1,w}\big(T^i, R_{j-1}(T)(P(\xi_j) - P(T))\big) \\ &= \sum_{\ell=1}^{h} a_{j,\ell} B_{h-1,w}(T^i, R_{j+\ell-1}(T)), \end{aligned}$$

and therefore that

$$P(\xi_j)\mathbf{z}_j = \sum_{\ell=1}^{h} a_{j,\ell}\mathbf{z}_{j+\ell}.$$

Applying this relation to all minors of order $h$ of $N_{h-1}^{(j)}$ which include the column $\mathbf{z}_j$ and using the multilinearity of the determinant, this gives

$$\begin{aligned} |P(\xi_j)|_w \|N_{h-1}^{(j)}\|_w &\le \max\Big\{|P(\xi_j)|_w, \sum_{\ell=1}^{h} |a_{j,\ell}|_w\Big\} \|N_{h-1}^{(j+1)}\|_w \\ &\ll \|P\|_w \|N_{h-1}^{(j+1)}\|_w. \end{aligned} \tag{22}$$

Combining these relations for $j = 1, \dots, t$, we get

$$\prod_{j=1}^{t} \frac{|P(\xi_j)|_w}{\|P\|_w} \le \frac{\|N_{h-1}^{(t+1)}\|_w}{\|N_{h-1}\|_w}.$$

On the other hand, since $\deg(P) \le h \le k \le n$, the estimates of the two preceding lemmas give

$$\|N_{h-1}^{(t+1)}\|_w \ll \big(\max_{j>t} \|\mathbf{z}_j\|_w\big)^h \ll X^{-h} \le X^{-\deg(P)}$$

and

$$\|N_{h-1}\|_w \gg \mathrm{H}(M_{h-1}) \gg \mathrm{H}(P)^{n-2h+2} \ge \mathrm{H}(P)^{n-2k+2}.$$

So, if $i$ denotes an index for which $|P(\xi_i)|_w$ is minimal, we find

$$\left(\frac{|P(\xi_i)|_w}{\|P\|_w}\right)^t \ll X^{-\deg(P)}\mathrm{H}(P)^{-(n-2k+2)}.$$

By multiplicativity, it follows that at least one irreducible factor $Q$ of $P$ has the same property. □

## 8. Degree and height estimates

The notation being the same as in the previous section, our goal is now to provide estimates for the degree and height of the polynomial $Q$ constructed in Lemma 7.3. We start with the following construction of an auxiliary polynomial (compare with [14, Prop. 7.2]).

**Lemma 8.1.** *Let the notation be as in Lemma 7.3. Then, there exists a constant $c_{14}$ with $0 < c_{14} < 1$ such that the following properties hold.*

(i) *Suppose that, for some integer $u \geq 0$, we have*

$$(XY)^{t+su} \leq c_{14}X^{n-2k+3}. \tag{23}$$

*Then there exists a non-zero polynomial $G \in E_{n-2k+2}$ of height at most $X$ such that $G^{(j)}$ belongs to $V_{k-1}$ for $j = 0, \dots, u$.*

(ii) *Suppose that, for some integer $u \geq 0$, we have*

$$(XY)^{t+u} \leq c_{14}X^{n-2k+3}, \tag{24}$$

*Suppose moreover that $\xi_1, \dots, \xi_t$ are all distinct, that we have $\xi_1 \notin K$ and $t \geq 2$, and that there exists a polynomial $A \in K[T]$ of degree 1 such that $\xi_{i+1} = A(\xi_i)$ for $i = 1, \dots, t-1$. Then there exists a non-zero polynomial $G \in E_{n-2k+2}$ of height at most $X$ such that $G \circ A^j$ belongs to $V_{k-1}$ for $j = 0, \dots, u$, where $A^j$ denotes the $j$-th iterate of $A$.*

*Proof.* The result follows from the adelic Minkowski convex body theorem applied to an adelic convex body $\mathcal{K} = \prod_v \mathcal{K}_v$ of $E_{n-2k+2}$ that we construct as follows, subject to the choice of a real number $c$ with $0 < c \leq 1$.

In the case (i), we put $\mathcal{S} = \mathcal{M}_\infty$. For each $v \in \mathcal{M} \setminus \{w\}$, we define $\mathcal{K}_v$ to be the set of elements $G$ of $E_{n-2k+2,v}$ with

$$\|G\|_v \leq \begin{cases} 1 & \text{if } v \notin \mathcal{S}, \\ c & \text{if } v \in \mathcal{S}, \end{cases} \tag{25}$$

and we define $\mathcal{K}_w$ to be the set of polynomials $G \in E_{n-2k+2,w}$ satisfying

$$\|G\|_w \leq cX \quad \text{and} \quad |G^{(j)}(\eta_i)|_w \leq cY^{-1} \quad (1 \leq i \leq s,\ 0 \leq j \leq m_i + u - 1).$$

We choose $c$ small enough, as a function of $n$ and $\max_{1\leq i\leq t} |\xi_i|_w$, so that, for each $G \in \mathcal{K}$, the products $T^\ell G^{(j)}(T)$ with $0 \leq \ell \leq k-1$ and $0 \leq j \leq u$ all belong to the interior of $\mathcal{C}(X, Y)$. Then, for a suitable choice of $c_{14}$, the condition (23) ensures that the volume of $\mathcal{K}$ is large enough so that, by Proposition 3.1, $\mathcal{K}$ contains a non-zero polynomial $G$ of $E_{n-2k+2}$. For

such a polynomial, we have $\mathrm{H}(G) \le X$ and, by the remark following the proof of Proposition 3.2, we get

$$\varphi(T^\ell G^{(j)}(T), \mathbf{y}) = 0 \quad (0 \le \ell \le k-1,\ 0 \le j \le u)$$

which shows that $G^{(j)} \in V_{k-1}$ for $j = 0, \dots, u$.

In the case (ii), the hypotheses $A(\xi_1) = \xi_2$ and $\xi_1 \notin K$ imply that $A \in K + KT$ is uniquely determined by $\xi_1$ and $\xi_2$. We denote by $\mathcal{S}$ the union of $\mathcal{M}_\infty$ with the finite set of places $v \in \mathcal{M}$ for which $\|A\|_v > 1$. For each $v \in \mathcal{M} \setminus \{w\}$, we define $\mathcal{K}_v$ to be the set of elements $G$ of $E_{n-2k+2,v}$ satisfying (25), and we define $\mathcal{K}_w$ to be the set of all polynomials $G \in E_{n-2k+2,w}$ satisfying

$$\|G\|_w \le cX \quad \text{and} \quad |(G \circ A^j)(\xi_1)|_w \le cY^{-1} \quad (0 \le j \le t+u-1).$$

In this situation, we choose $c$ depending only on $n$, $\max_{v\in\mathcal{M}} \|A\|_v$ and $\max_{1\le i\le t} |\xi_i|_w$ so that, for each $G \in \mathcal{K}$, the products $T^\ell (G \circ A^j)(T)$ with $0 \le \ell \le k-1$ and $0 \le j \le u$ all belong to the interior of $\mathcal{C}(X, Y)$. Then, as in the preceding case, a suitable choice of $c_{14}$ in the condition (24) ensures that $\mathcal{K}$ contains a non-zero polynomial $G$ of $E_{n-2k+2}$, and any such polynomial $G$ has the requested properties. □

We conclude with the following result.

**Lemma 8.2.** *Suppose that the conditions (i) or (ii) of Lemma 8.1 are fulfilled for some integer $u \ge 0$ and that, in the case (ii), we have $A^j(T) \ne T$ for $j = 0, \dots, n-2k+2$. Then, under the hypotheses of Lemma 7.3, the irreducible polynomial $Q$ of $K[T]$ produced by Lemma 7.3 has*

$$\deg(Q) \le \frac{n-2k+2}{u+1} \quad \text{and} \quad \mathrm{H}(Q) \le c_{15} X^{1/(u+1)}. \tag{26}$$

*Proof.* Let $G$ be as in the conclusion of Lemma 8.1. Since $Q$ is an irreducible factor of a polynomial $P$ which by Lemma 7.2 divides any element of $V_{k-1}$, the polynomial $Q$ divides $G^{(j)}$ for $j = 0, \dots, u$ in the case (i), and $G \circ A^j$ for $j = 0, \dots, u$ in the case (ii). In the case (i), we deduce that $Q^{u+1}$ divides $G$ and the estimates (26) follow.

In the case (ii), the polynomials $Q, Q \circ A^{-1}, \dots, Q \circ A^{-u}$ are irreducible factors of $G$ of the same degree, and we have

$$c^{-j}\mathrm{H}(Q) \le \mathrm{H}(Q \circ A^{-j}) \le c^j \mathrm{H}(Q) \quad (0 \le j \le u),$$

for a constant $c \ge 1$ depending only on $n$ and $\mathrm{H}(A)$. Since the relation $A(\xi_1) = \xi_2$ determines uniquely $A$, this constant $c$ ultimately depends only on $n$, $\xi_1$ and $\xi_2$. Let $m$ be the largest integer with $1 \le m \le u+1$ such that $Q, Q \circ A^{-1}, \dots, Q \circ A^{-(m-1)}$ are two by two relatively prime. Then, the product $\prod_{j=0}^{m-1} Q \circ A^{-j}$ divides $G$ and we deduce that

$$m \deg(Q) \le \deg(G) \quad \text{and} \quad \mathrm{H}(Q)^m \ll \mathrm{H}(G). \tag{27}$$

If $m = u+1$, this gives (26). Assume now that $m \le u$. Then $Q \circ A^m$ is a multiple of $Q$ and therefore $A^m$ permutes the roots of $Q$. In particular, there exist a root $\alpha$ of $Q$ and an

integer $i$ with $1 \le i \le \deg(Q)$ such that $A^{mi}(\alpha) = \alpha$. Then, $Q$ divides $A^{mi}(T) - T$. By hypothesis, the latter polynomial is non-zero since by (27) we have $mi \le n - 2k + 2$. Hence, $Q$ has degree 1 and its height is equal to that of $A^{mi}(T) - T$. This again gives (26) upon noting that the condition (24) implies $u + 1 \le n - 2k + 2$ (since $X, Y \ge 1$ and $c_{14} < 1$). $\square$

## 9. Proof of the main Proposition 6.1

Let the notation and hypotheses be as in the statement of Theorem 2.1 (resp. Theorem 2.2). Define accordingly $\nu = 4Dst$ (resp. $\nu = 4t$) as in the statement of Proposition 6.1. Define also $k = [(n+2)t/\nu]$ where the brackets denote the integer part. Since $n \ge \nu \ge 4t$, this integer $k$ satisfies

$$t \le k \le \min\{n/2, (n - t + 2)/2\}.$$

We also note that, in the situation of Theorem 2.2, the point $(\xi_1, \dots, \xi_t)$ is a zero of the prime ideal $\mathfrak{p}$ of $K[x_1, \dots, x_t]$ generated by the polynomials $x_{i+1} - A(x_i)$ for $i = 1, \dots, t-1$. To be consistent with the notation of Theorem 2.1, we then put $D = 1$, since this ideal $\mathfrak{p}$ has degree 1. In both cases, we define $u = Dt$. We also denote by $\xi$ the point of $\mathbb{P}^t(\mathbb{C}_w)$ with homogeneous coordinates $\underline{\xi} = (1, \xi_1, \dots, \xi_t)$, and by $\mathfrak{P}$ the homogeneous prime ideal of $K[x_0, \dots, x_t]$ which is mapped to $\mathfrak{p}$ under the specialization $x_0 \mapsto 1$.

Assume, by contradiction, that the conclusion of the proposition does not hold and define $Y$ as a function of $X$ by $Y = X^{(n+2-\nu)/\nu}$. Then, there exists a real number $X_0 \ge 1$ such that, for each $X \ge X_0$, the convex body $\mathcal{C}^{\varphi}(X, Y)$ defined in §6 contains a non-zero point $\mathbf{y}$ of $K^{n+1}$. Then, assuming that $X_0$ is sufficiently large, all conditions of Lemmas 7.2, 7.3, 8.1 and 8.2 are fulfilled. Indeed, for $X$ sufficiently large, we find

$$c_{11}(XY)^t = c_{11}X^{(n+2)t/\nu} < X^{k+1},$$

and so the main condition $c_{11}Y^t < X^{k+1-t}$ of Lemma 7.2 is satisfied. We also find

$$(XY)^{t+su} = X^{(n+2)t(1+Ds)/\nu} \le X^{(n+2)/2} \quad \Big( \text{ resp. } (XY)^{t+u} = X^{(n+2)/2} \Big),$$

while $n - 2k + 3 > (n+2)/2$. So, the main condition (23) (resp. (24)) of Lemma 8.1 is satisfied for each sufficiently large $X$. Thus, assuming $X_0$ sufficiently large, Lemma 7.3 provides, for each $X \ge X_0$, an irreducible polynomial $Q = Q_X$ of $K[T]$ and an index $i = i_X$ with $1 \le i \le t$ such that

$$\left( \frac{|Q(\xi_i)|_w}{\|Q\|_w} \right)^t \le c_{13} X^{-\deg(Q)} \mathrm{H}(Q)^{-(n-2k+2)}. \tag{28}$$

By Lemma 8.2, this polynomial satisfies

$$\deg(Q) \le \frac{n - 2k + 2}{u + 1} \quad \text{and} \quad \mathrm{H}(Q) \le c_{15} X^{1/(u+1)}.$$

Moreover, since $[K(\xi_i) : K] \ge n/u > \deg(Q)$, we also have $Q(\xi_i) \ne 0$. Define

$$n' = \left[ \frac{n - 2k + 2}{u + 1} \right] \quad \text{and} \quad Y = c_{15} X^{1/(u+1)},$$

and let $P = P_Y$ denote the homogeneous polynomial of $K[x_0, \dots, x_t]$ with the same degree as $Q$, for which $P(1, x_1, \dots, x_t) = Q(x_i)$. Then, $P$ has degree at most $n'$ and height at most $Y$. It does not belong to $\mathfrak{P}$ since it does not vanish at the point $\xi$. Moreover, by (28), we have

$$\frac{|P(\underline{\xi})|_w}{\|P\|_w \|\underline{\xi}\|_w^{\deg(P)}} \ll X^{-\deg(P)/t} \mathrm{H}(P)^{-(n-2k+2)/t} \ll Y^{-1/t} \left( Y^{\deg(P)} \mathrm{H}(P)^{n'} \right)^{-D}$$

so that, for any sufficiently large value of $Y$, the above polynomial $P_Y = P$ satisfies the main hypothesis (29) of Theorem A.1 below, with $n$ replaced by $n'$. This is a contradiction as none of these polynomials vanish at $\xi$.

## Appendix A. A version of Gel'fond's criterion for curves

In this appendix, we denote by $\mathbb{C}_w$ the completion of $\bar{K}$ with respect to its unique absolute value (also denoted $|\ |_w$) which extends $|\ |_w$ on $K$. Then, $\mathbb{C}_w$ is an algebraically closed field containing $K_w$ as a subfield. We also fix a positive integer $t$ and, for conciseness, we put $K[\mathbf{x}] = K[x_0, \dots, x_t]$ where $x_0, \dots, x_t$ denote independent variables over $K$. We denote by $\deg(P)$ the degree of a homogeneous polynomial $P$ of $K[\mathbf{x}]$ and by $\mathrm{H}(P)$ its height, that is the height of the vector of its coefficients. Similarly, for a homogeneous ideal $I$ of $K[\mathbf{x}]$, we denote by $\deg(I)$ its degree and by $\mathrm{H}(I)$ the height of a Chow form of $I$ (see below for a precise definition). Our goal is to prove the following result which generalizes Theorem 4.2 of [14] (see also Theorem 2b of [6]).

**Theorem A.1.** *Let $n$ be a positive integer, let $\mathfrak{P}$ be a homogeneous prime ideal of $K[\mathbf{x}]$ whose zero set $\overline{V}$ in $\mathbb{P}^t(\mathbb{C}_w)$ has dimension 1, let $D = \deg(\mathfrak{P})$, and let $\underline{\xi} = (\xi_0, \dots, \xi_t)$ be homogeneous coordinates of a point $\xi$ of $\overline{V}$. Suppose that, for any sufficiently large real number $Y \geq 1$, there exists a homogeneous polynomial $P = P_Y \in K[\mathbf{x}]$ of degree at most $n$ and height at most $Y$ which does not belong to $\mathfrak{P}$ and satisfies*

$$\frac{|P(\underline{\xi})|_w}{\|P\|_w \|\underline{\xi}\|_w^{\deg(P)}} < e^{-24t^3n^2D} \mathrm{H}(\mathfrak{P})^{-n^2} \left( \mathrm{H}(P)^n Y^{\deg(P)} \right)^{-D}. \tag{29}$$

*Then the point $\xi$ is defined over an algebraic extension of $K$ of degree at most $nD$ and the above polynomials vanish at this point for any sufficiently large $Y$.*

Our proof follows essentially the arguments of P. Philippon in §II.3 of [13], taking advantage of a simpler context. For convenience, we base this proof on the formalism and results of Yu. V. Nesterenko in [12]. We start by recalling the notion of a Chow form of a homogeneous ideal $I$ of $K[\mathbf{x}]$ and related concepts which, in view of our present choice of normalization for the absolute values of $K$ (see §2), differ slightly from those of [12].

Let $u_{i,j}$ for $i = 1, \dots, t+1$ and $j = 0, \dots, t$ be independent variables over $K[\mathbf{x}]$, and write $\mathbf{u}_i = (u_{i,0}, \dots, u_{i,t})$ for $i = 1, \dots, t+1$. Let $I$ be a homogeneous ideal of $K[\mathbf{x}]$, let $Z$ denote the set of zeros of $I$ in $\mathbb{P}^t(\mathbb{C}_w)$, and put $r = \dim(Z) + 1$ with the convention that $r = 0$ if $Z$ is

empty. Denote by $I(r)$ the ideal of $K[\mathbf{x}, \mathbf{u}_1, \dots, \mathbf{u}_r]$ generated by the elements of $I$ and the polynomials $u_{i,0}x_0 + \cdots + u_{i,t}x_t$ for $i = 1, \dots, r$, and denote by $\bar{I}(r)$ the ideal of $K[\mathbf{u}_1, \dots, \mathbf{u}_r]$ consisting of the elements $G$ of that ring for which there exists an integer $M \geq 1$ such that $Gx_j^M \in I(r)$ for $j = 0, \dots, t$. Then $\bar{I}(r)$ is a non-zero principal ideal and we define a Chow form of $I$ to be any generator $F$ of this ideal (see §1 of [12] for other denominations and an historical perspective). It is known that such a polynomial of $K[\mathbf{u}_1, \dots, \mathbf{u}_r]$ is separately homogeneous of degree $\deg(I)$ in each set of variables $\mathbf{u}_1, \dots, \mathbf{u}_r$. Moreover, as $F$ is uniquely determined up to multiplication by a non-zero element of $K$, it makes sense (in view of the product formula) to define the *height* $\mathrm{H}(I)$ of $I$ to be the height $\mathrm{H}(F)$ of the vector of coefficients of $F$.

Let $S^{(1)}, \dots, S^{(r)}$ be skew symmetric matrices of order $t+1$ whose coefficients above the diagonal are altogether independent variables over $\mathbb{C}_w$, and let $\kappa$ denote the $K$-linear ring homomorphism from $K[\mathbf{u}_1, \dots, \mathbf{u}_r]$ to $\mathbb{C}_w[S^{(1)}, \dots, S^{(r)}]$ mapping $\mathbf{u}_i$ to $\underline{\xi}S^{(i)}$ for $i = 1, \dots, r$. Following [12], we define the absolute value of $I$ at $\xi$ by

$$|I(\xi)|_w = \frac{\|\kappa(F)\|_w}{\|F\|_w \|\underline{\xi}\|_w^{r\deg(I)}},$$

where $\|F\|_w$ (resp. $\|\kappa(F)\|_w$) stands for the largest absolute value of the coefficients of F (resp. $\kappa(F)$). This is independent of the choice of $F$ as well as the choice of homogeneous coordinates $\underline{\xi}$ for $\xi$. Moreover, we have $|I(\xi)|_w = 0$ if and only if $\xi$ belongs to an irreducible component of $Z$ of dimension $r-1$.

Finally, we define the distance between $\xi$ and a point $z$ of $\mathbb{P}^t(\mathbb{C}_w)$ with projective coordinates $\mathbf{z} = (z_0, \dots, z_t)$ by the formula

$$\mathrm{dist}(\xi, z) = \|\underline{\xi}\|_w^{-1} \|\mathbf{z}\|_w^{-1} \max_{0 \leq j,k \leq t} |\xi_j z_k - \xi_k z_j|_w$$

(again this is independent of the choices of coordinates $\underline{\xi}$ for $\xi$ and $\mathbf{z}$ for $z$). Accordingly, we define the distance between $\xi$ and the set $Z$ of zeros of $I$ in $\mathbb{P}^t(\mathbb{C}_w)$ by

$$\mathrm{dist}(\xi, Z) = \inf\{\mathrm{dist}(\xi, z)\,;\, z \in Z\}.$$

We can now state the results of [12] that we need.

**Lemma A.2.** *Let $J$ be an unmixed homogeneous ideal of $K[x_0, \dots, x_t]$ and let $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ be its associated prime ideals. Then, there exist integers $k_1, \dots, k_s \geq 1$ such that*

(i) $\sum_{j=1}^s k_j \deg(\mathfrak{p}_j) \leq \deg(J)$,
(ii) $\prod_{j=1}^s \mathrm{H}(\mathfrak{p}_j)^{k_j} \leq e^{t^2 \deg(J)} \mathrm{H}(J)$,
(iii) $\prod_{j=1}^s |\mathfrak{p}_j(\underline{\xi})|_w^{k_j} \leq e^{t^3 \deg(J)} |J(\underline{\xi})|_w$.

This follows immediately from a simple adaptation of the proof of Proposition 1.2 of [12] upon noting that, for each Archimedean place $v \in \mathcal{M}_\infty$, the absolute value $|\ |_v^{d/d_v}$ of $K$ coincides with the usual absolute Archimedean value on $\mathbb{Q}$ and that we have $\sum_{v \in \mathcal{M}_\infty} d_v/d =$

1. Then, the local estimates of [12] applied to the absolute values $|\ |_v^{d/d_v}$ with $v \in \mathcal{M}_\infty$ combine to give assertion (ii) and lead to a stronger form of the assertion (iii) where the argument of the exponential is replaced by $(d_w/d)t^3 \deg(J)$.

**Lemma A.3.** *Let $\mathfrak{q}$ be a homogeneous prime ideal of $K[\mathbf{x}]$ whose zero set $Z$ in $\mathbb{P}^t(\mathbb{C}_w)$ is not empty, and let $P$ be a homogeneous polynomial from $K[\mathbf{x}]$ with $P \notin \mathfrak{q}$. Put*

$$r = \dim(Z) + 1, \quad \rho = \operatorname{dist}(\xi, Z) \quad \text{and} \quad \delta = \frac{|P(\underline{\xi})|_w}{\|P\|_w \|\underline{\xi}\|_w^{\deg(P)}}.$$

*If $r \geq 2$, there exists a homogeneous unmixed ideal $J$ of $K[\mathbf{x}]$ with the following properties. Its set of zeros in $\mathbb{P}^t(\mathbb{C}_w)$ has dimension $r-2$ and coincide with that of $(\mathfrak{q}, P)$. Moreover, we have:*

(i) $\deg(J) \leq \deg(\mathfrak{q}) \deg(P)$,

(ii) $\mathrm{H}(J) \leq e^{2t^2 \deg(\mathfrak{q}) \deg(P)} \mathrm{H}(\mathfrak{q})^{\deg(P)} \mathrm{H}(P)^{\deg(\mathfrak{q})}$,

(iii) $|J(\underline{\xi})|_w \mathrm{H}(J) \leq e^{11t^2 \deg(\mathfrak{q}) \deg(P)} \mathrm{H}(\mathfrak{q})^{\deg(P)} \mathrm{H}(P)^{\deg(\mathfrak{q})} \begin{cases} \delta & \text{if } \rho < \delta, \\ |\mathfrak{q}(\underline{\xi})|_w & \text{otherwise.} \end{cases}$

*If $r = 1$, the above inequality (iii) holds with the left hand side replaced by 1.*

This second result follows from a similar adaptation of the proof of Proposition 1.4 of [12]. Part (ii) uses moreover $r + 1 \leq 2t$ while part (iii) requires replacing the inequality (37) on page 314 of [12] with an equality involving the height of the given Chow form $G$ of $J$.

**Corollary A.4.** *Let $\mathfrak{q}$ and $P$ be as in Lemma A.3. Then, any minimal prime ideal $\mathfrak{p}$ of $(\mathfrak{q}, P)$ satisfies*

$$\deg(\mathfrak{p}) \leq \deg(\mathfrak{q}) \deg(P) \quad \text{and} \quad \mathrm{H}(\mathfrak{p}) \leq e^{3t^2 \deg(\mathfrak{q}) \deg(P)} \mathrm{H}(\mathfrak{q})^{\deg(P)} \mathrm{H}(P)^{\deg(\mathfrak{q})}.$$

*Proof.* Lemma A.3 provides a homogeneous unmixed ideal $J$ of $K[\mathbf{x}]$ whose minimal prime ideals are the same as those of $(\mathfrak{q}, P)$. Since the degree of any ideal is bounded below by 0 while its height is bounded below by 1, Lemma A.2 then shows that each minimal prime ideal $\mathfrak{p}$ of $(\mathfrak{q}, P)$ satisfies $\deg(\mathfrak{p}) \leq \deg(J)$ and $\mathrm{H}(\mathfrak{p}) \leq e^{t^2 \deg(J)} \mathrm{H}(J)$. The conclusion follows using the upper bounds for $\deg(J)$ and $\mathrm{H}(J)$ provided by Lemma A.3 (i) and (ii). □

*Proof of Theorem A.1.* Choose $Y_0 \geq 1$ such that $P_Y$ is defined for each $Y \geq Y_0$. Then fix an arbitrary choice of $Y$ with $Y \geq Y_0$ and put $P = P_Y$. Since $P \notin \mathfrak{P}$ and since $\operatorname{dist}(\xi, \overline{V}) = 0$, Lemma A.3 provides us with a homogeneous unmixed ideal $J$ of $K[\mathbf{x}]$ whose set of zeros in $\mathbb{P}^t(\mathbb{C}_w)$ has dimension 0 and coincide with that of $(\mathfrak{P}, P)$. The same lemma also gives estimates for this ideal, which taking into account the inequality (29) and the fact that $\deg(P) \leq n$, imply $\deg(J) \leq D \deg(P) \leq nD$ and

$$\begin{aligned} |J(\underline{\xi})|_w \mathrm{H}(J)^n &\leq e^{11t^2 n^2 D} \mathrm{H}(\mathfrak{P})^{n^2} \mathrm{H}(P)^{nD} \frac{|P(\underline{\xi})|_w}{\|P\|_w \|\underline{\xi}\|_w^{\deg(P)}} \\ &< e^{-13t^3 n^2 D} Y^{-D \deg(P)}. \end{aligned}$$

Let $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ be the associated prime ideals of $J$ in $K[\mathbf{x}]$. According to lemma A.2, there exist integers $k_1, \dots, k_s \geq 1$ such that $\sum_{j=1}^s k_j \deg(\mathfrak{p}_j) \leq \deg(J)$ and

$$\prod_{j=1}^s \big(|\mathfrak{p}_j(\underline{\xi})|_w \mathrm{H}(\mathfrak{p}_j)^n\big)^{k_j} \leq e^{t^2(t+n)\deg(J)} |J(\underline{\xi})|_w \mathrm{H}(J)^n.$$

Putting these estimates together, we get

$$\prod_{j=1}^s \big(|\mathfrak{p}_j(\underline{\xi})|_w \mathrm{H}(\mathfrak{p}_j)^n\big)^{k_j} < \big(e^{-11t^2n} Y^{-1}\big)^{\deg(J)} \leq \prod_{j=1}^s \big(e^{-11t^2n} Y^{-1}\big)^{k_j \deg(\mathfrak{p}_j)}.$$

Therefore, there is at least one index $j$ for which the prime ideal $\mathfrak{p} = \mathfrak{p}_j$ satisfies

$$|\mathfrak{p}(\underline{\xi})|_w < e^{-11t^2nN} \mathrm{H}(\mathfrak{p})^{-n} Y^{-N} \quad \text{where } N = \deg(\mathfrak{p}). \tag{30}$$

Now, define $X_0$ as the infimum of all real numbers $X$ with $X \geq Y_0$ such that $P_X \in \mathfrak{p}$. By construction, we have $Y_0 \leq X_0 \leq Y$. Moreover, for each $X \geq X_0$ such that $P_X \in \mathfrak{p}$, the ideal $\mathfrak{p}$ is a minimal prime ideal of $(\mathfrak{P}, P_X)$. Therefore, Corollary A.4 gives

$$\mathrm{H}(\mathfrak{p}) \leq e^{3t^2 D \deg(P_X)} \mathrm{H}(\mathfrak{P})^{\deg(P_X)} \mathrm{H}(P_X)^D \leq e^{3t^2nD} \mathrm{H}(\mathfrak{P})^n X^D.$$

As $X$ can be taken arbitrarily close to $X_0$, this implies

$$\mathrm{H}(\mathfrak{p}) \leq e^{3t^2nD} \mathrm{H}(\mathfrak{P})^n X_0^D. \tag{31}$$

Assume for the moment that $Y_0 < X_0$. Choose $X$ with $\max\{Y_0, X_0/2\} \leq X < X_0$ and put $Q = P_X$. Define also

$$\rho = \mathrm{dist}(\xi, Z) \quad \text{and} \quad \delta = \frac{|Q(\underline{\xi})|_w}{\|Q\|_w \|\underline{\xi}\|^{\deg(Q)}}$$

where $Z$ denotes the zero set of $\mathfrak{p}$ in $\mathbb{P}^t(\mathbb{C}_w)$. Since $Q \notin \mathfrak{p}$ and $\dim(Z) = 0$, the inequality of Lemma A.3 (iii) applies with the left hand side replaced by 1, $\mathfrak{q}$ replaced by $\mathfrak{p}$, and $P$ replaced by $Q$. If $\rho < \delta$, then, taking into account (31) together with $N \leq nD$, $\deg(Q) \leq n$ and $X_0 \leq 2X$, this gives

$$1 \leq e^{11t^2nN} \mathrm{H}(\mathfrak{p})^{\deg(Q)} \mathrm{H}(Q)^N \delta \leq e^{15t^2n^2D} \mathrm{H}(\mathfrak{P})^{n^2} X^{D\deg(Q)} \mathrm{H}(Q)^{nD} \delta$$

against the upper bound for $\delta$ associated with $Q = P_X$. So, we have $\rho \geq \delta$ and Lemma A.3 (iii) then gives

$$1 \leq e^{11t^2nN} \mathrm{H}(\mathfrak{p})^{\deg(Q)} \mathrm{H}(Q)^N |\mathfrak{p}(\underline{\xi})|_w.$$

which now contradicts (30) since $\deg(Q) \leq n$ and $\mathrm{H}(Q) \leq X \leq Y$.

Thus, we have $X_0 = Y_0$ which in view of (31) means that the height of $\mathfrak{p}$ is bounded above by a constant which is independent of $Y$. Since the degree of $\mathfrak{p}$ is bounded by $nD$, this implies that, as $Y$ varies, $\mathfrak{p}$ stays within a finite set of ideals. Since the upper bound for $|\mathfrak{p}(\underline{\xi})|_w$ given by (30) tends to zero as $Y$ tends to infinity, this shows that $|\mathfrak{p}(\underline{\xi})|_w = 0$ for any sufficiently large $Y$ and thus that $\xi$ is a zero of $\mathfrak{p}$ for those values of $Y$. In particular,

we deduce that $\xi$ is defined over an algebraic extension of $K$ of degree at most $nD$ and that $P_Y(\xi) = 0$ for any sufficiently large $Y$. □

## References


[1] Y. Bugeaud, O. Teulié, Approximation d'un nombre réel par des nombres algébriques de degré donné, *Acta Arith.* **93** (2000), 77-86.

[2] E. B. Burger, Homogeneous Diophantine approximation in $S$-integers, *Pacific J. Math.* **152** (1992), 211–253.

[3] E. Bombieri and J. Vaaler, On Siegel's lemma, *Invent. Math.* **73** (1983), 11–32.

[4] J. W. S. Cassels, Global fields, Chapter II in: *Algebraic number theory*, J. W. S. Cassels and A. Fröhlich editors, Academic Press, 1967.

[5] E. Dubois, Théorèmes de transfert en géométrie des nombres sur un anneau d'adèles de $\mathbb{Q}$, *C. R. Acad. Sci. Paris Sér. A*, **283** (1976), 803–806.

[6] H. Davenport and W. M. Schmidt, Approximation to real numbers by algebraic integers, *Acta Arith.* **15** (1969), 393–416.

[7] M. Laurent, Simultaneous rational approximation to the successive powers of a real number, *Indag. Math. (N.S.)* **11** (2003), 45–53.

[8] M. Laurent and D. Roy, Criteria of algebraic independence with multiplicities and approximation by hypersurfaces, *J. reine angew. Math.* **536** (2001), 65–114.

[9] K. Mahler, Inequalities for ideal bases in algebraic number fields, *J. Austral. Math. Soc.* **4** (1964), 425–448.

[10] R. B. Macfeat, Geometry of numbers in adele spaces, *Dissertationes Math. (Rozprawy Mat.)* **88** (1971), 54 pp.

[11] J. F. Morrison, Approximation of $p$-adic numbers by algebraic numbers of bounded degree, *J. Number Theory* **10** (1978), 334–350.

[12] Yu. V. Nesterenko, On the measure of algebraic independence of the values of the Ramanujan functions, Tr. Mat. Inst. Steklova **218** (1997), 299–334 (Russian); English translation in Proc. Steklov Inst. Math. **218** (1997), 294–331.

[13] P. Philippon, Critères pour l'indépendance algébrique, *Pub. Math. IHES* **64** (1986), 5-52.

[14] D. Roy and M. Waldschmidt, Diophantine approximation by conjugate algebraic integers, *Compositio Math.* **140** (2004), 593–612.

[15] W. M. Schmidt, *Diophantine approximation*, Lecture Note in Math., vol. 785, Springer-Verlag, 1980.

[16] O. Teulié, Approximation d'un nombre $p$-adique par des nombres algébriques, *Acta Arith.* **102** (2002), 137–155.

[17] E. Wirsing, Approximation mit algebraischen Zahlen beschränkten Grades, *J. reine angew. Math.* **206** (1961), 67-77.



Département de Mathématiques, Université d'Ottawa, 585 King Edward, Ottawa, Ontario K1N 6N5, Canada

*E-mail address*: droy@uottawa.ca